



Version 5.2 Migration Guide

Version 5.2
August 18, 2015

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

Cisco Systems, Inc.

www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2015 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

| | |
|--|------------|
| Introduction to Version 5.2 | 1-1 |
| Cisco® Security Migration Services | 1-2 |
| New and Changed Terminology | 1-2 |
| New, Changed, and Updated Features and Functionality | 1-3 |
| Device Management | 1-4 |
| Licensing | 1-4 |
| Redundancy and Resource Sharing | 1-15 |
| Network Traffic Management | 1-16 |
| Access Control | 1-16 |
| Intrusion Detection and Prevention | 1-19 |
| File Tracking, File Control, and Malware Protection | 1-19 |
| Network Discovery | 1-21 |
| Geolocation Information | 1-21 |
| Dashboards | 1-22 |
| Context Explorer | 1-22 |
| Reusable Objects | 1-22 |
| Reporting | 1-23 |
| Health Monitoring | 1-23 |
| Client Vulnerabilities and VDB Updates | 1-23 |
| User Certificates | 1-23 |
| IPv6 Support | 1-23 |
| Application Programming Interfaces | 1-24 |
| Deprecated Functionality | 1-24 |
| Appliance Series, Models, and Capabilities | 1-25 |
| Series 2 Appliances | 1-25 |
| Series 3 Appliances | 1-26 |
| Virtual Appliances | 1-26 |
| Supported Capabilities by Appliance Model | 1-26 |
| Where Do I Begin? | 1-28 |
| For More Information | 1-29 |

CHAPTER 2

| | |
|---|------------|
| Understanding the Migration Process | 2-1 |
| CAUTION: Do Not Interrupt the Reimage Process | 2-2 |

- Migrating a Simple Multi-Sensor Deployment **2-3**
 - Migrating Configurations to a Replacement Defense Center **2-5**
 - Migrating 3D Sensors **2-6**
 - Migrating Events from Defense Center to Defense Center **2-10**
- Performing a Multi-Sensor Rolling Migration **2-11**
- Migrating Stacked 3D Sensors **2-13**
- Migrating By Reimaging the Existing Defense Center **2-14**
 - Exporting Configurations and Events from the Defense Center **2-15**
 - Completing the Migration Using the Sensor Migration Script **2-16**
 - Completing the Migration Manually **2-21**
- Migrating a Deployment with a Virtual Defense Center **2-24**
- Migrating High Availability Defense Center Pairs **2-25**
 - Replacing Paired Defense Centers **2-26**
 - Migrating an Existing High Availability Pair of Defense Centers **2-26**
- Migrating Standalone 3D Sensors with IPS **2-27**

CHAPTER 3

Preparing for Migration 3-1

- Appliance, Version, and License Requirements **3-2**
 - Supported Appliances **3-2**
 - Supported Source and Destination Versions for the Migration **3-3**
 - SEU and Intrusion Rule Update Requirements **3-3**
 - Version 5.2 License Requirements **3-4**
 - Disk Space Requirements **3-5**
 - Configuration and Event Backup Guidelines **3-5**
- Time and Physical Access Requirements **3-5**
- Traffic Flow and Inspection During the Migration **3-6**
- Addressing Configuration Incompatibilities **3-7**
 - Multiple Same-Type Detection Engines Using One Interface Set **3-8**
 - Intrusion Policy Proliferation Due To Custom Variables **3-8**
 - Errors Due to Unavailable Policies **3-9**
 - RNA Port Exclusion Issues **3-10**
 - Unsupported RNA and RUA Fast-Path PEP Rules **3-10**
 - Unsupported Conditions in Compliance Rules and Traffic Profiles **3-11**
 - Intrusion Rules with Ports Have No Service Metadata **3-11**
- Obtaining and Installing Migration Packages **3-12**

CHAPTER 4

Performing the Migration 4-1

- Logging Into an Appliance to Run Migration Scripts **4-2**

| | |
|--|------|
| Exporting Configurations from a Version 4.10.3 Appliance | 4-3 |
| Exporting Events from a Version 4.10.3 Appliance | 4-6 |
| Importing Configurations onto a Version 5.2 Defense Center | 4-7 |
| Starting the Configuration Import Script | 4-8 |
| Reviewing the Manifest of Exported Configurations | 4-9 |
| Verifying Configuration Incompatibilities | 4-9 |
| Resolving Configuration Conflicts | 4-10 |
| Creating Security Zones Based on Interface Sets | 4-13 |
| Providing Basic Access Control Settings | 4-15 |
| Verifying the Migrated Configuration | 4-16 |
| Confirming the Import and Resolving Configuration Collisions | 4-16 |
| Configuration Import Script Syntax and Options | 4-17 |
| Importing Configurations Multiple Times | 4-18 |
| Importing Events onto a Version 5.2 Defense Center | 4-20 |
| Rebuilding Version 4.10.3 Appliances | 4-21 |
| Reimaging and Registering Devices with the Sensor Migration Script | 4-22 |
| Manually Adding Version 5.2 Devices to the Defense Center | 4-31 |
| Completing Your Version 5.2 Deployment | 4-33 |
| Configuring and Verifying Sensing Interfaces and Inline Sets | 4-33 |
| Applying Network Discovery and Access Control Policies | 4-38 |
| Next Steps | 4-39 |

CHAPTER 5

| | |
|--|------------|
| Understanding Migrated Configurations and Events | 5-1 |
| Understanding the New Access Control Policy | 5-2 |
| Migrating PEP Rules into Access Control Rules | 5-3 |
| Migrating Intrusion Policies and Creating Access Control Rules | 5-4 |
| Migrating RNA Settings into Rules and Logging Preferences | 5-7 |
| Example Migrated Access Control Rules | 5-10 |
| Understanding How Interface Sets Become Security Zones | 5-12 |
| Understanding How RNA and RUA Settings Are Migrated | 5-13 |
| Understanding How The Migration Creates Discovery Rules | 5-14 |
| Migrating Other RNA and RUA Settings | 5-16 |
| Understanding Migrated Intrusion and Audit Events | 5-18 |
| Understanding Migrated Compliance Policies and Rules | 5-18 |
| Changes to eStreamer Syntax and Data Structures | 5-19 |



Introduction to Version 5.2

Version 5.0 introduced a large new feature set which was further expanded in subsequent releases. Regardless of model, appliances running Version 4.10.x of the system **cannot** be updated directly to Version 5.x. To update, you must reimage your physical appliances and re-create your virtual appliances, which results in a loss of all stored events and most configuration data.

For your convenience, Cisco provides the following export, import, and sensor migration scripts:

- Four scripts allow you to export configurations and events from a Version 4.10.3.x (patch 4.10.3.5 or later) Defense Center® or standalone sensor and import them onto a Version 5.2.0.x Defense Center:
 - configuration export script
 - configuration import script
 - event export script
 - event import script
- A sensor migration script allows you to remotely reimage up to twenty (ten maximum recommended) Version 4.10.3 (or a later patch) Series 2 and Series 3 sensors in parallel to Version 5.2 using a Version 5.2.0.x Defense Center. Note that it is not necessary to update sensors from Version 4.10.3 to 4.10.3.5 to use the sensor migration script.

Before you begin the migration process for your deployment you **must** make sure you have a detailed plan and that you have fully prepared your appliances, including obtaining and installing the new licenses, resolving issues that could prevent a clean migration, setting up replacement appliances, installing the migration scripts, and so on. Although Cisco recommends you perform the migration in a maintenance window or at a time when the interruption will have the least impact on your deployment, the migration process can take a significant amount of time. You can minimize disruption by thoroughly preparing, but it is unlikely you will be able to avoid it completely.



Caution

Failure to plan and prepare could cause a longer than expected disruption to your deployment during the migration.

The topics that follow introduce you to Version 5.2, including its differences from earlier versions. For differences in a release subsequent to Version 5.2, see the release notes for that version.

- [Cisco® Security Migration Services, page 1-2](#)
- [New and Changed Terminology, page 1-2](#)
- [New, Changed, and Updated Features and Functionality, page 1-3](#)
- [Deprecated Functionality, page 1-24](#)

- [Appliance Series, Models, and Capabilities](#), page 1-25
- [Where Do I Begin?](#), page 1-28

Cisco® Security Migration Services

Cisco® Security Migration Services help customers move from Version 4.x software to Version 5.x. Cisco will perform an analysis of the current environment, develop a migration plan, test the plan in a lab, and perform the migration in the production environment. With detailed planning and careful change management, we help ensure that your security solution protects the infrastructure while meeting your business needs. Contact your Cisco account representative to order Cisco Security Migration Services.

New and Changed Terminology

Due to the many new and changed features introduced in Version 5.0 through Version 5.2, the terminology in both the software and its documentation has changed accordingly. To ensure maximum ease of use and familiarity with Version 5.2, review these changes carefully.

The table below contains a brief overview of the most important changed terms. For more information on new and changed features, see the next sections in this chapter. For detailed definitions of both new and changed terms, see the glossary in the [Version 5.2 Sourcefire 3D System User Guide](#).

Table 1-1 Terminology Changes

| This term in Version 4.10.3 | Is now this term in Version 5.2 |
|--|---|
| IPS, RNA, RUA, PEP | These technologies have been fully integrated into the system and are no longer referred to separately. |
| 3D Sensor, sensor | device, managed device |
| SEU (Security Enhancement Update) | rule update, intrusion rule update, SRU (rarely) |
| client application | client, client application (rarely) |
| service | application protocol, server (when there is an associated vendor and version) |
| payload (discovery) | web application |
| flow (as a general term and before data, event, graph, summary, tracker) | connection |
| compliance (before event, policy, rule), Policy and Response | correlation Note that the term compliance, when referring to compliance white lists, remains in use. |
| Default Dashboard | Summary Dashboard |
| RNA detection policy | network discovery policy |
| RNA detector | application detector |
| RNA event | discovery event |
| RNA Recommended Rules | FireSIGHT recommendations |
| RUA Agent | User Agent |
| RUA event | user activity |

Table 1-1 Terminology Changes (continued)

| This term in Version 4.10.3 | Is now this term in Version 5.2 |
|---------------------------------------|------------------------------------|
| RUA user | user, user identity |
| report profile | report template |
| system settings | local configuration |
| fail-open (interface protection mode) | bypass (interface set bypass mode) |

New, Changed, and Updated Features and Functionality

The Version 5.2 web interface is streamlined and improved; it is significantly different from Version 4.10.3 releases. The look and feel is updated, many terms have changed, and new menus and options support new functionality.

New predefined dashboards, new workflows, and a reorganized host profile present your network assets in a manner consistent with the new features and terminology changes. Predefined user roles have changed to reflect the overall organization of the system and the web interface.

For Series 3 and virtual devices, Version 5.2 includes CLI commands that correspond with the new features and functionality and removes commands that are no longer needed. If you enable Simple Network Management Protocol (SNMP) polling, there are new counters in the management information base (MIB) files for managed devices that include traffic statistics associated with the new features.

The following sections summarize the new, changed, and updated functionality that you will encounter when you migrate a deployment to Version 5.2:

- [Device Management, page 1-4](#)
- [Licensing, page 1-4](#)
- [Redundancy and Resource Sharing, page 1-15](#)
- [Network Traffic Management, page 1-16](#)
- [Access Control, page 1-16](#)
- [Intrusion Detection and Prevention, page 1-19](#)
- [File Tracking, File Control, and Malware Protection, page 1-19](#)
- [Network Discovery, page 1-21](#)
- [Geolocation Information, page 1-21](#)
- [Dashboards, page 1-22](#)
- [Context Explorer, page 1-22](#)
- [Reusable Objects, page 1-22](#)
- [Reporting, page 1-23](#)
- [Health Monitoring, page 1-23](#)
- [Client Vulnerabilities and VDB Updates, page 1-23](#)
- [User Certificates, page 1-23](#)
- [IPv6 Support, page 1-23](#)
- [Application Programming Interfaces, page 1-24](#)

Device Management

In Version 5.2, only essential management and monitoring functions are available on managed devices. Almost all configuration and analysis functions are restricted to the Defense Center, including the configuration of the new features available in Version 5.2.

Standalone 3D Sensors used as an intrusion detection and prevention system (IPS) are no longer supported. Use the migration feature to transfer intrusion policies and events from your standalone 3D Sensor with IPS to a Version 5.2 Defense Center.

Licensing

Your organization can license a variety of features to create an optimal deployment. Version 5.2 uses a different licensing scheme than Version 4.10.3. Most licenses from previous releases are not supported. You must use the Defense Center to control licenses for itself and the devices it manages.



Tip

Add licenses during the initial setup of your Version 5.2 Defense Centers. Otherwise, any devices you register during initial setup are added to the Defense Center as unlicensed. You must then enable licenses on each device individually after the initial setup process is over. For more information, see the [Sourcefire 3D System Installation Guide, Version 5.2](#).

For more information, see:

- [Host and User Licenses, page 1-4](#)
- [Feature Licenses, page 1-5](#)
- [Using the Product Upgrade Tool, page 1-7](#)
- [Selecting PIDs for Upgrade Licenses, page 1-13](#)
- [Selecting PIDs for Additional Feature Licenses, page 1-14](#)
- [Additional Information, page 1-15](#)
- [Configuring and Verifying Sensing Interfaces and Inline Sets, page 4-33](#)

Host and User Licenses

In Version 5.2, a FireSIGHT license is required to perform host, application, and user discovery. The FireSIGHT license on your Defense Center also determines how many individual hosts and users you can monitor with the Defense Center and its managed devices, as well as how many users you can use to perform user control. FireSIGHT host and user license limits are model-specific, as listed in the following table.

Table 1-2 FireSIGHT Limits by Defense Center Model

| Defense Center Model | FireSIGHT Host and User Limit |
|----------------------|-------------------------------|
| DC500 | 1000 (no user control) |
| DC750 | 2000 |
| DC1000 | 20,000 |
| DC1500 | 50,000 |

Table 1-2 *FireSIGHT Limits by Defense Center Model (continued)*

| Defense Center Model | FireSIGHT Host and User Limit |
|----------------------|-------------------------------|
| DC3000 | 100,000 |
| DC3500 | 300,000 |

When you migrate your deployment to Version 5.2, you can use your legacy RNA Host and RUA User licenses instead of a FireSIGHT license. Version 5.2 Defense Centers with legacy licenses use the RNA Host limit as the FireSIGHT host limit and the RUA User limit as both the FireSIGHT user and access-controlled user limit.

**Tip**

During the Version 4.10.3 to Version 5.2 manual reimage process of a physical appliance, you are prompted to delete license and management interface network settings. Keep these settings, although you can re-add them later if you accidentally delete them. For more information, see the [Version 5.2 Sourcefire 3D System Installation Guide](#).

RNA Host and RUA User limits are cumulative. That is, you can add multiple licenses of each type to the Defense Center to monitor the total number of hosts or users allowed by the licenses.

If you later add a FireSIGHT license, the Defense Center uses the higher of the limits. For example, the FireSIGHT license on the DC1500 supports up to 50,000 hosts and users. If the RNA Host limit on your Version 4.10.3 DC1500 was higher than 50,000, using that legacy host license on the same Defense Center running Version 5.2 gives you the higher limit. For your convenience, the web interface displays only the licenses that represent the higher limits.

**Note**

Because FireSIGHT license limits are matched to the hardware capabilities of Defense Centers, Cisco does **not** recommend exceeding them when using legacy licensing. For guidance, contact Support.

Feature Licenses

Model-specific licenses allow your managed devices to perform a variety of functions, as follows:

Protection

A Protection license allows managed devices to perform intrusion detection and prevention, file control, and Security Intelligence filtering. Note you do not enable a Protection license on Series 2 devices. Registering a Series 2 device to a Version 5.2 Defense Center automatically enables intrusion detection and prevention and file control, without a license. Security Intelligence is not supported on Series 2 devices.

Control

A Control license allows Series 3 managed devices to perform user and application control. It also allows devices to perform switching and routing (including DHCP relay), NAT, and to cluster devices and stacks. A Control license requires a Protection license.

URL Filtering

A URL Filtering license allows Series 3 managed devices to use regularly updated cloud-based category and reputation data to determine which traffic can traverse your network, based on the URLs requested by monitored hosts. A Version 5.2 URL Filtering license also requires Protection and Control licenses.

Malware

A Malware license allows Series 3 managed devices to perform network-based advanced malware protection (AMP), that is, to detect and block malware in files transmitted over your network. It also allows you to view trajectories, which track files transmitted over your network. A Malware license requires a Protection license.

VPN

A VPN license allows you to build secure VPN tunnels among the virtual routers on Series 3 managed devices, or from managed devices to remote devices. A VPN license requires Protection and Control licenses.

Because of architecture and resource limitations, not all licenses can be applied to all managed devices. In general, you cannot license a capability that a device does not support; see [Table 1-4 on page 1-27](#).

The following table summarizes which licenses you can add to your Defense Center and apply to each device model. The Defense Center rows (for all licenses except FireSIGHT) indicate whether that Defense Center can manage devices using those licenses. For example, you can use a Series 2 DC1000 to create a VPN deployment using Series 3 devices, but you cannot use a DC500 to perform category and reputation-based URL filtering, regardless of the devices it manages. Note that n/a marks Defense Center-based licenses that are not relevant to managed devices.

Table 1-3 Supported Licenses by Model

| Models | FireSIGHT or RNA/RUA | Protection | Control | URL Filtering | Malware | VPN |
|--|----------------------|---|----------------------------------|---------------|---------|-----|
| Series 2 devices: <ul style="list-style-type: none"> 3D500/1000/2000 3D2100/2500/3500/4500 3D6500 | n/a | no license required; all Protection capabilities automatically granted except Security Intelligence, which is not supported | no | no | no | no |
| Series 3 devices: <ul style="list-style-type: none"> 7000 Series 8000 Series | n/a | yes | yes | yes | yes | yes |
| virtual devices | n/a | yes | no support for hardware features | yes | yes | no |
| DC500 Series 2 Defense Center | yes | no Security Intelligence | no user control | no | no | yes |
| DC1000/3000 Series 2 Defense Centers | yes | yes | yes | yes | yes | yes |
| DC750/1500/3500 Series 3 Defense Centers | yes | yes | yes | yes | yes | yes |
| virtual Defense Centers | yes | yes | yes | yes | yes | yes |

Using the Product Upgrade Tool

This section explains how to use the self-service Cisco Product Upgrade Tool to acquire FireSIGHT and Control perpetual licenses for \$0 when migrating from 4.10 to 5.x. These licenses are necessary to enable all the base functionality of the FireSIGHT Management Center (previously referred to as the *Defense Center*) and any FirePOWER Appliances it manages (previously referred to as *managed devices*).

Note the following:

- The Control upgrade license that you get using the Product Upgrade Tool also provides the capabilities of the Protection license.
- FirePOWER 5.x does not support standalone devices, so all sensor appliances running Version 5.x must be managed via a FireSIGHT Management Center.

To use the PUT tool to order upgrade licenses:

- Step 1** Login to the Product Upgrade Tool (<http://tools.cisco.com/gct/Upgrade/jsp/index.jsp>) using your CCO ID.

Product Upgrade Tool

HOME

HOW TO BUY

Product Upgrade Tool

News and Enhancements

User Guides

Questions and Answers

Glossary

New Product Search

Start Product Upgrade

Enter Contract number and select method to upgrade.

Contract Number

94713860

Guided

This method provides with step-by-step process to upgrade.

Advanced

Use this method if you know exactly which upgrade product to order.

Continue

408171

- Step 2** Enter the service contract number 94713860 **EXACTLY AS SHOWN** and select the **Continue** button. **YOU MUST USE THIS SERVICE CONTRACT NUMBER. YOU CANNOT SUBSTITUTE ANY OTHER NUMBER.**

Guided Method

Contract Number → **Upgrade Selection** → Upgrade SKU

Select Product Group *Required Field

Product Group* Current Version* Upgrade Version*

SOURCEFIRE Version 4.X Version5.X

Back Continue

403172

- Step 3** Under Product Group, click on **SOURCEFIRE**. Under Current Version, click on **Version 4.X**. Under Upgrade Version click on **Version 5.X**. Select **Continue** in the lower right corner.

Guided Method

Upgrade SKU

Add another upgrade or continue to complete your order.

L-3D2500-5UPG-K9=
Cisco Software Upgrade from 4.x to 5.x for 3D2500

SF-FSVMW-5UPG-K9
Cisco FireSIGHT 4.x to 5.x Upgrade PID

L-3D1000-5UPG-K9=
Cisco Software Upgrade from 4.x to 5.x for 3D1000

Add Another Upgrade Continue

403173

- Step 4** On the Upgrade SKU page, select **Continue** in the lower right corner.

Guided Method

Upgrade Summary

Select Delivery Option and enter quantity of product upgrades.
Some products are not available for eDelivery.

| Product Number | Special Ordering Note | License Key Requested | Delivery Option | Quantity |
|---|-----------------------|---|--|----------------------|
| L-3D1000-5UPG-K9= | | <input type="radio"/> Single <input checked="" type="radio"/> Multiple | <input type="radio"/> Physical <input checked="" type="radio"/> eDelivery | <input type="text"/> |
| Cisco Software Upgrade from 4.x to 5.x for 3D1000 ⓘ | | | | |
| L-3D2000-5UPG-K9= | | <input type="radio"/> Single <input checked="" type="radio"/> Multiple | <input type="radio"/> Physical <input checked="" type="radio"/> eDelivery | <input type="text"/> |
| Cisco Software Upgrade from 4.x to 5.x for 3D2000 ⓘ | | | | |
| L-3D2100-5UPG-K9= | | <input type="radio"/> Single <input checked="" type="radio"/> Multiple | <input type="radio"/> Physical <input checked="" type="radio"/> eDelivery | <input type="text"/> |
| Cisco Software Upgrade from 4.x to 5.x for 3D2100 ⓘ | | | | |

403174

- Step 5** Specify the delivery option and quantity you need for each upgrade license shown, then select **Continue** in the lower right corner. See [Selecting PIDs for Upgrade Licenses, page 1-13](#) for more information regarding which PID(s) to select.

Guided Method

Shipping Details

Shipping Contact *Required Field

Shipping Address



Add a Shipping Address...*

Enter your **Technical Assistance Center (TAC)** or **Customer Service (SR)** case number, if applicable.

TAC/SR Case Number:

eDelivery Email:*

Optionally you can fill notes to provide any additional information.

Carton Notes:

[Copy to Ordering Notes](#)

[Copy to Shipping Notes](#)

Order Processing Notes:

[Copy to Shipping Notes](#)

Shipping & Packaging Notes:

Additional E-mail

Enter additional email addresses that you wish to receive for confirmation of your order.

Additional E-mail

Note: Multiple email addresses can be entered using comma, e.g. xxx@yyy.zzz, aaa@bbb.ccc.

Back

Continue

403175

- Step 6** Enter your shipping address & shipping contact. Click on **Add a Shipping Address** and scroll down to the bottom to select your address or add an address. .
- Step 7** Enter your **TAC/SR Case Number** (if applicable), **eDelivery Email**, **Additional Email** addresses (if applicable), **Carton Notes**, **Order Processing Notes**, and **Shipping & Packaging Notes**. Select **Continue** in the lower right corner.
- Step 8** Please read and agree to the Product Upgrade Tool – Software Ordering Rules.
- Step 9** Review your order detail for correctness and select **Submit Order**.
- Step 10** You will receive an email confirmation of your order and an order acknowledgment with an estimated shipping date once the order is scheduled.



New Request

Thank you for placing your order.
Your Online Order ID is **UG442994**

An e-mail confirmation of your order has been automatically sent to **ES@ES.COM**.

403176

- Step 11** Once the order has been fulfilled, you will receive either an email or a physical paper Claim Certificate, depending on the delivery preference you selected while ordering.
- Step 12** If you received a Claim Certificate, skip to *To register and fulfill a license through Cisco*.

To download your Claim Certificate when you receive an eDelivery Email:

- Step 1** Open the email confirming your order.

Product Upgrade Tool

[HOME](#)

[Start Product Upgrade](#)

[HOW TO BUY](#)

Enter Contact number and select method to upgrade

- Step 2** Scroll down the email until you see the box titled *eDelivery Access Order*. Select the **eDelivery Access Order** link at the bottom.

eDelivery

Order Based Access

[Send Order Based Access Email](#)

| | | |
|-----------------------|---------------|------------|
| Cisco SO | 100278161 | Bill-To PO |
| Carton/Cust Ref Notes | Test Not Real | |

Products Ordered

| | |
|--|---|
| <input type="checkbox"/> L-3D2100-5UPG-K9= (QTY - 1) | Cisco Software Upgrade from 4.x to 5.x for 3D2100 |
| Description | Test Not Real |
| Carton/Cust Ref Line Notes | Test Not Real |

[Download Selected](#) [Download All Licenses](#) [Download Entire Order](#)

403178

- Step 3** Click the plus sign under Products Ordered.

| L-3D2100-5UPG-K9= (QTY - 1) | | | | | | Status | Downloaded |
|---|-----------|-----------------|-------------------|---|------------|-----------|------------|
| Description | | | | | | Available | 03/11/15 |
| Carton/Cust Ref Line Notes | | | | | | | |
| Cisco Software Upgrade from 4.x to 5.x for 3D2100 | | | | | | | |
| Test Not Real | | | | | | | |
| Select All Deselect All | | | | | | | |
| | Line ID | File Type | Product ID | Description | Status | QT | |
| <input type="checkbox"/> | 926033752 | License | L-3D2100-5UPG-K9= | Cisco Software Upgrade from 4.x to 5.x for 3D2100 | Downloaded | 1 | |
| <input type="checkbox"/> | | License (Claim) | | LIC,Generic Software Claim Certificate, 7x8.5" | Downloaded | 1 | ↓ |

Step 4 Click the green arrow.

License Agreement Confirmation

You must accept the [End User License Agreement](#) to download this software.

Accept License Agreement
 Decline License Agreement

License Download Cart

[Download All Licenses](#)

| <input type="checkbox"/> | Order # | Line ID | Product ID | File Type | Description | QT | |
|-------------------------------------|-----------|-----------|-------------------|-----------------|--|----|------------------------|
| <input checked="" type="checkbox"/> | 100278161 | 926033752 | L-3D2100-5UPG-K9= | License (Claim) | LIC,Generic Software Claim Certificate, 7x8.5" | 1 | Remove |

[Delete Selected Licenses from Cart](#)

Step 5 Select **Accept License Agreement**. In the License Download Cart, select the check box of the claim certificate to download. Click **Download All Licenses**.

Step 6 Save the zip file to your desktop, which includes an End User License Agreement and your Claim Certificate, which includes your PAK number.

To register and fulfill a license through Cisco:

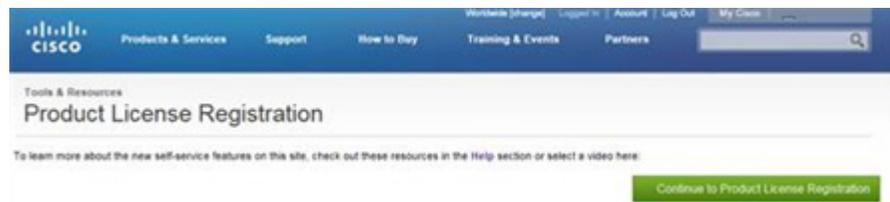
To register your Product Authorization Key and obtain a license, please follow the steps below:

Step 1 Go to www.cisco.com/go/license.

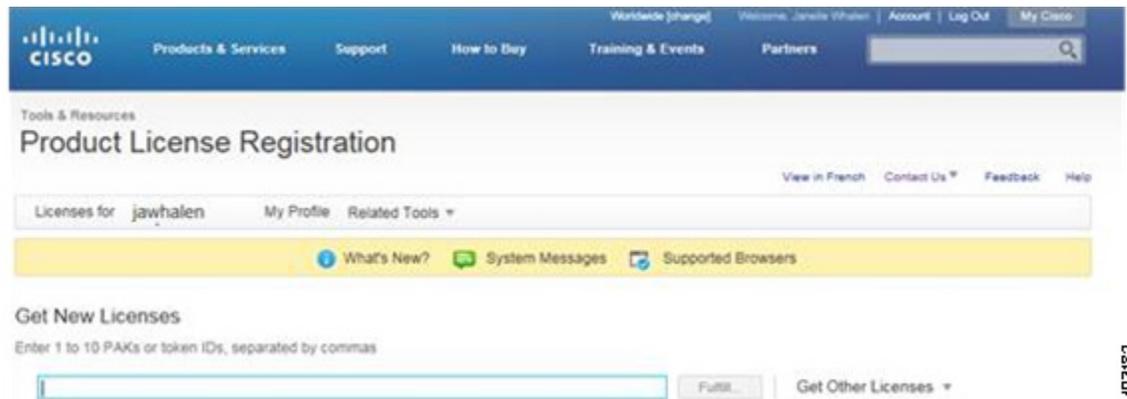


Note

You will need a CCO ID to access the License Registration Portal.



Step 2 Click the green **Continue to Product License Registration** button on the right-hand side of the screen.



- Step 3** Enter the Cisco PAK into the **Get New Licenses** text box and click the **Fulfill** box.
- Step 4** Your license is generated on the screen as well as emailed to you directly.

Selecting PIDs for Upgrade Licenses

Use this table to select PIDs to use with the Product Upgrade Tool.

| Need a Protection and Control OR FireSIGHT License for: | Select Below: | For Reference by Partners and Account teams only | | |
|---|-------------------|--|-----------------------|--------------------------------------|
| Model | Upgrade Licenses | Source Fire PID | Cisco Equivalent PIDs | Description |
| 3D500 | L-3D500-5UPG-K9= | 3D500-IPS-C04-000 | FP500-PROT-LIC | |
| 3D1000 | L-3D1000-5UPG-K9= | 3D1000-IPS-C04-000 | FP1000-PROT-LIC | |
| 3D2000 | L-3D2000-5UPG-K9= | 3D2000-IPS-C04-000 | FP2000-PROT-LIC | |
| 3D2100 | L-3D2100-5UPG-K9= | 3D2100-IPS-C04-000 | FP2100-PROT-LIC | |
| 3D2500 | L-3D2500-5UPG-K9= | 3D2500-IPS-C04-F04 | FP2500-PROT-LIC | |
| 3D3500 | L-3D3500-5UPG-K9= | 3D3500-IPS-C04-F04 | FP3500-PROT-LIC | |
| 3D4500 | L-3D4500-5UPG-K9= | 3D4500-IPS-C04-F04 | FP4500-PROT-LIC | |
| 3D6500 | L-3D6500-5UPG-K9= | 3D6500-IPS-C06-F02-LR | FP6500-PROT-LIC | |
| FP7010 | L-FP7010-5UPG-K9= | LIC-CTRL-3D7010 | FP7010-CTRL-LIC | Cisco FirePOWER 7010 Control License |
| FP7020 | L-FP7020-5UPG-K9= | LIC-CTRL-3D7020 | FP7020-CTRL-LIC | Cisco FirePOWER 7010 Control License |
| FP7030 | L-FP7030-5UPG-K9= | LIC-CTRL-3D7030 | FP7030-CTRL-LIC | Cisco FirePOWER 7010 Control License |
| FP7110 | L-FP7110-5UPG-K9= | LIC-CTRL-3D7110 | FP7110-CTRL-LIC | Cisco FirePOWER 7010 Control License |
| FP7120 | L-FP7120-5UPG-K9= | LIC-CTRL-3D7120 | FP7120-CTRL-LIC | Cisco FirePOWER 7010 Control License |

| Need a Protection and Control OR FireSIGHT License for: | Select Below: | For Reference by Partners and Account teams only | | |
|---|-------------------|--|-----------------------|--------------------------------------|
| Model | Upgrade Licenses | Source Fire PID | Cisco Equivalent PIDs | Description |
| FP8120 | L-FP8120-5UPG-K9= | LIC-CTRL-3D8120 | FP8120-CTRL-LIC | Cisco FirePOWER 7010 Control License |
| FP8130 | L-FP8130-5UPG-K9= | LIC-CTRL-3D8130 | FP8130-CTRL-LIC | Cisco FirePOWER 7010 Control License |
| FP8140 | L-FP8140-5UPG-K9= | LIC-CTRL-3D8140 | FP8140-CTRL-LIC | Cisco FirePOWER 7010 Control License |
| FP8250 | L-FP8250-5UPG-K9= | LIC-CTRL-3D8250 | FP8250-CTRL-LIC | Cisco FirePOWER 7010 Control License |
| FP8260 | L-FP8260-5UPG-K9= | LIC-CTRL-3D8260 | FP8260-CTRL-LIC | Cisco FirePOWER 7010 Control License |
| FP8270 | L-FP8270-5UPG-K9= | LIC-CTRL-3D8270 | FP8270-CTRL-LIC | Cisco FirePOWER 7010 Control License |
| FP8290 | L-FP8290-5UPG-K9= | LIC-CTRL-3D8290 | FP8290-CTRL-LIC | Cisco FirePOWER 7010 Control License |
| Virtual FirePOWER | L-FPVMW-5UPG-K9= | V3D-RedHat-IPS-1 | FP-VM-RH-IPS-LIC= | |
| | | V3D-VMWARE-IPS-1 | FP-VMW4-IPS-LIC= | |
| | | V3D-XEN-IPS-1 | FP-VM-XEN-IPS-LIC= | |
| | | LIC-CTRL-VMWARE | FP-VMW-IPS-LIC | |
| | | V3D-NGFW-VMWARE | | |
| FireSIGHT License for management center on v5.x | SF-FSVMW-5UPG-K9 | VDC-RedHat | FS-VM-REDHAT-SW-K9 | |
| | | VDC-VMWARE | FS-VMW-SW-K9 | |
| | | VDC-XEN | FS-VMW-XEN-SW-K9 | |
| | | VDC-64bit-VMWARE-BNDL-0 | FS-VMW-SW-K9 | |
| | | VDC-VMWARE-FS410-0 | FS410X-VMW-SW-K9 | |
| | | VDC-XEN-FS410-0 | FS-VM-XEN-MAX-K9 | |

Selecting PIDs for Additional Feature Licenses

Use this table to select PIDs for ordering subscription licenses for additional features. See [Cisco Security Ordering Guide for Legacy Sourcefire and Related Cisco Offerings](#) for more information.

| Model | IPS+Apps+SI | IPS+Apps+SI & Advanced Malware Protection | IPS+Apps+SI & URL Filtering | IPS+Apps+SI & URL Filtering & Advanced Malware Protection |
|--------|----------------|---|-----------------------------|---|
| 3D500 | FP500-TA-LIC= | n/a | n/a | n/a |
| 3D1000 | FP1000-TA-LIC= | n/a | n/a | n/a |
| 3D2000 | FP2000-TA-LIC= | n/a | n/a | n/a |

| Model | IPS+Apps+SI | IPS+Apps+SI & Advanced Malware Protection | IPS+Apps+SI & URL Filtering | IPS+Apps+SI & URL Filtering & Advanced Malware Protection |
|-------------------|----------------|---|-----------------------------|---|
| 3D2100 | FP2100-TA-LIC= | n/a | n/a | n/a |
| 3D2500 | FP2500-TA-LIC= | n/a | n/a | n/a |
| 3D3500 | FP3500-TA-LIC= | n/a | n/a | n/a |
| 3D4500 | FP4500-TA-LIC= | n/a | n/a | n/a |
| 3D6500 | FP6500-TA-LIC= | n/a | n/a | n/a |
| FP7010 | FP7010-TA-LIC= | FP7010-TAM-LIC= | FP7010-TAC-LIC= | FP7010-TAMC-LIC= |
| FP7020 | FP7020-TA-LIC= | FP7020-TAM-LIC= | FP7020-TAC-LIC= | FP7020-TAMC-LIC= |
| FP7030 | FP7030-TA-LIC= | FP7030-TAM-LIC= | FP7030-TAC-LIC= | FP7030-TAMC-LIC= |
| FP7110 | FP7110-TA-LIC= | FP7110-TAM-LIC= | FP7110-TAC-LIC= | FP7110-TAMC-LIC= |
| FP7120 | FP7120-TA-LIC= | FP7120-TAM-LIC= | FP7120-TAC-LIC= | FP7120-TAMC-LIC= |
| FP8120 | FP8120-TA-LIC= | FP8120-TAM-LIC= | FP8120-TAC-LIC= | FP8120-TAMC-LIC= |
| FP8130 | FP8130-TA-LIC= | FP8130-TAM-LIC= | FP8130-TAC-LIC= | FP8130-TAMC-LIC= |
| FP8140 | FP8140-TA-LIC= | FP8140-TAM-LIC= | FP8140-TAC-LIC= | FP8140-TAMC-LIC= |
| FP8250 | FP8250-TA-LIC= | FP8250-TAM-LIC= | FP8250-TAC-LIC= | FP8250-TAMC-LIC= |
| FP8260 | FP8260-TA-LIC= | FP8260-TAM-LIC= | FP8260-TAC-LIC= | FP8260-TAMC-LIC= |
| FP8270 | FP8270-TA-LIC= | FP8270-TAM-LIC= | FP8270-TAC-LIC= | FP8270-TAMC-LIC= |
| FP8290 | FP8290-TA-LIC= | FP8290-TAM-LIC= | FP8290-TAC-LIC= | FP8290-TAMC-LIC= |
| Virtual FirePOWER | FPVMW-TA-LIC= | FPVMW-TAM-LIC= | FPVMW-TAC-LIC= | FPVMW-TAMC-LIC= |

Additional Information

Watch the [License Activation Video](#) for a demonstration.

You can find additional information on licensing in the [Sourcefire Licensing Support Forum](#).

Redundancy and Resource Sharing

The redundancy and resource-sharing features allow you to ensure continuity of operations and to combine the processing resources of multiple physical devices. Device stacking and Defense Center high availability are still supported on many models. Version 5.2 adds clustering, clustered stacks, and other methods of achieving Layer 3 redundancy.

Defense Center High Availability

To ensure continuity of operations, a Defense Center *high availability* feature allows you to designate redundant DC1000, DC1500, DC3000, or DC3500 Defense Centers to manage devices. The new configurations available in Version 5.2 are maintained on peer Defense Centers. Additionally, the Vulnerability Database (VDB) is now synchronized.

Device Stacking

Device stacking allows you to increase the amount of traffic inspected on a network segment by connecting two to four physical devices in a stacked configuration. When you establish a stacked configuration, you combine the resources of each stacked device into a single, shared configuration. The same devices that supported stacking in Version 4.10.3 support it in Version 5.2.

Device Clustering

Device clustering (sometimes called device high availability) allows you to establish redundancy of networking functionality and configuration data between two or more Series 3 devices or stacks. Clustering two or more peer devices or stacks results in a single logical system for policy applies, system updates, and registration. With device clustering, the system can fail over either manually or automatically.

SFRP

In most cases, you can achieve Layer 3 redundancy without clustering devices by using the Sourcefire Redundancy Protocol (SFRP). SFRP allows Series 3 devices to act as redundant gateways for specified IP addresses. With network redundancy, you can configure two or more devices or stacks to provide identical network connections, ensuring connectivity for other hosts on the network.

Network Traffic Management

Version 5.2 has multiple network traffic management features that allow licensed Series 3 devices to act as part of your organization's network infrastructure. You can:

- configure a Layer 2 deployment to perform packet switching between two or more network segments
- configure a Layer 3 deployment to route traffic between two or more interfaces
- enable strict enforcement for an inline set, virtual router, or virtual switch on a physical managed device, which blocks connections where the three-way handshake is incomplete
- perform network address translation (NAT)
- build secure VPN tunnels from virtual routers on managed devices to remote devices

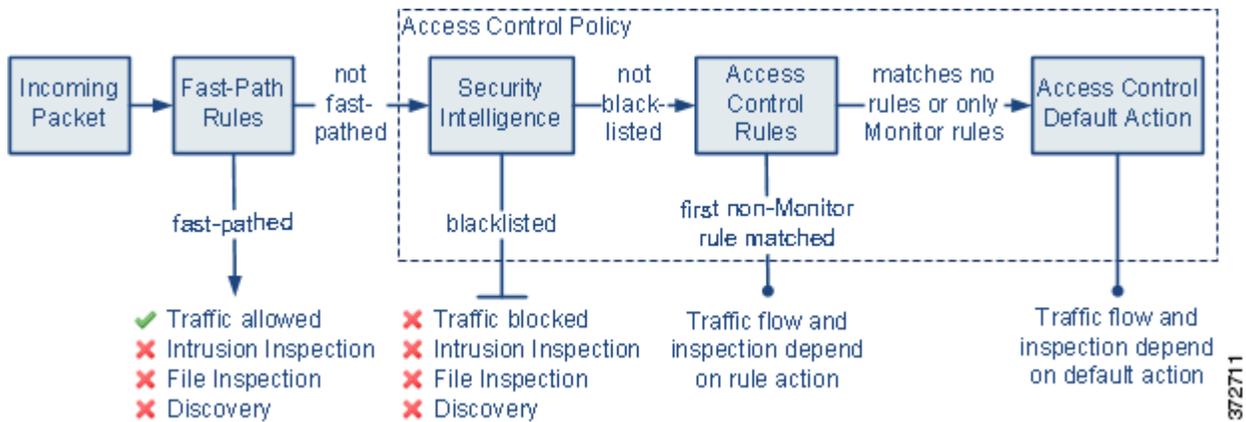
Access Control

Access control is a new policy-based feature that allows you to specify, inspect, and log the traffic that can traverse your network. An *access control policy* determines how the system handles traffic on your network.

Access control rules inside a policy define how traffic is handled by managed devices. These rules can allow, monitor, inspect, or block traffic based on multiple criteria. They can perform simple IP matching, or create complex scenarios involving different networks, users, applications, ports, and URLs.

Using rules within access control policies, you can also invoke intrusion detection and prevention, file control, and advanced malware protection on specific traffic. Finally, access control policies define the traffic that you permit and, therefore, the traffic you can monitor with the discovery feature (previously called *RNA*).

The diagram below illustrates traffic flow through the system, and provides some details on the types of inspection performed on that traffic.



For more information, see:

- [Security Intelligence Filtering, page 1-17](#)
- [Application Control, page 1-17](#)
- [User Control, page 1-18](#)
- [URL Filtering, page 1-18](#)
- [Connection Logging, page 1-18](#)
- [Intrusion Detection and Prevention, page 1-19](#)
- [File Tracking, File Control, and Malware Protection, page 1-19](#)
- [Network Discovery, page 1-21](#)

Security Intelligence Filtering

As part of access control, *Security Intelligence* allows you to blacklist—deny traffic to and from—specific IP addresses before the traffic is subjected to analysis by access control rules.

Series 2 devices cannot perform Security Intelligence filtering, nor can the DC500 manage a Security Intelligence deployment.

Application Control

Application control allows you to use the application detection capabilities to determine the traffic that you want to block, allow, or inspect further. The system detects the following types of application:

- *application protocols* (formerly *services*) such as HTTP and SSH, which represent communications between hosts
- *clients* (formerly *client applications*) such as web browsers and email clients, which represent software running on the host
- *web applications* (formerly *payloads*) such as MPEG video and Facebook, which represent the content or requested URL for HTTP traffic

The system also associates each application that it detects with a predetermined risk and business relevance, as well as a category and optional tags that describe the application's functions and effects.

You can use access control to handle traffic based on the detection of individual applications, or for groups of applications called application filters (see [Reusable Objects, page 1-22](#)).

Series 2 devices cannot perform application control.

User Control

User control allows you to use the user detection capabilities, in conjunction with a Microsoft Active Directory deployment, to determine the traffic that you want to block, allow, or inspect. User control replaces and augments the Version 4.10.3 Real-Time User Awareness (RUA) component.

The Defense Center retrieves groups and user names from an Active Directory server you specify. *Sourcefire User Agents* (formerly *RUA Agents*) monitor those users as they log into the network or when they authenticate against Active Directory credentials for any other reason. You can handle network traffic for these *access-controlled users* on an individual or group basis.

You can also track (but not control) activity for *non-access-controlled users*, including users detected in specific types of network traffic (for example, IMAP or SIP/VoIP) by managed devices. User Agents can also report LDAP logins for *non-access-controlled users*, and the Defense Center can retrieve user metadata from Active Directory servers.



Note

Use at least Version 2.1 of the User Agent with your Version 5.2 deployment. Version 2.1 has flexible deployment options and includes IPv6 support. It also can detect logoffs and provide information on various types of logins, including interactive user logins to a host, remote desktop logins, file-share authentication, and computer account logins. Support for legacy agents will be phased out in future releases. For more information, see the [Sourcefire 3D System User Agent Configuration Guide](#).

Series 2 devices cannot perform user control, nor can the DC500 manage a user control deployment, although each of these appliances can gather user identity data.

URL Filtering

URL filtering is a licensed feature that allows you to determine the traffic that you want to block, allow, or inspect, based on URLs requested by monitored hosts.

When you enable URL filtering, the Defense Center contacts a cloud service, retrieves data on many commonly visited URLs, and saves that data on licensed appliances. Each of these URLs has an associated category and reputation. These attributes allow you to quickly create URL conditions for access control rules, which can group and combine URL categories and reputations.

Because the cloud service is continually updated with new URLs, as well as new categories and risks for existing URLs, using the cloud service ensures that the system uses up-to-date information to filter requested URLs. Malicious sites that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and apply new policies.

You can also achieve more granular, custom control over URL conditions in access control rules by specifying individual URLs or groups of URLs.

Series 2 devices cannot perform URL filtering of any kind. The DC500 cannot manage a deployment where you filter traffic by URL category and reputation. However, the DC500 can manage devices that filter web traffic using individual URLs or groups of URLs.

Connection Logging

In Version 5.2, you now use the access control feature (instead of the RNA detection policy) to configure the logging of *connection events* (formerly *flow data*) detected by managed devices.

For each access control rule, you must decide whether you want to log connections that match the rule. Tying connection logging to individual rules gives you granular control over the connections you want to log.

You should log connections according to the security and compliance needs of your organization. If your goal is to limit the number of events you generate, only enable logging for the traffic critical to your analysis. However, if you want a broader view of your network traffic, you can enable logging for additional rules.

Depending on the rule, you can log a connection event at the beginning or end of a matched connection, or both. In Version 4.10.3, RNA logged connection events only at the end of connections.

In general, if you want to perform analysis on connection data, log end-of-connection events. This is because beginning-of-connection events do not have information that must be determined by examining traffic over the duration of the session. If, however, you simply want to log an event each time the system detects a new connection, beginning-of-connection events are sufficient.

**Note**

As in previous releases, you configure NetFlow connection logging in the network discovery policy.

Intrusion Detection and Prevention

In Version 5.2, intrusion detection and prevention is integrated with access control. Instead of applying intrusion policies independently, you can now associate an intrusion policy with specific access control rules. When traffic matches an access control rule, the system uses the associated intrusion policy to inspect it. The system can also use an intrusion policy associated with the default action of an access control policy to inspect traffic that does not match rules in the policy.

Intrusion Rule Updates

Intrusion *rule updates*, sometimes called SRUs, replace Security Enhancement Updates (SEUs).

Rule updates provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. Rule updates may also delete rules and provide new rule categories and system variables. However, they no longer provide new or updated intrusion prevention features such as preprocessors.

FireSIGHT Rule Recommendations

If you use FireSIGHT rule recommendations, the system no longer makes intrusion rule state recommendations for rules with a very high overhead rating. Now, you must manually set the rule state for any rule with a very high overhead rating. If you have intrusion policies where the threshold is set to very high, the migration process changes it to high.

Adaptive Profiles

In Version 5.2, the system applies an intrusion rule to traffic if the rule's service metadata matches application traffic. This occurs regardless of whether you enable adaptive profiles. Enabling adaptive profiles still applies host information gathered from the network to traffic for processing.

File Tracking, File Control, and Malware Protection

To help you identify and mitigate the effects of malware, Version 5.2 of the system includes file control, network file trajectory, and advanced malware protection (AMP) components. You can detect, track, and optionally block the transmission of files (including malware files) in network traffic.

File Control

File control allows managed devices to detect and block your users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols. You configure file control as part of your overall access control configuration; file policies associated with access control rules inspect network traffic that meets rule conditions.

Network-Based Advanced Malware Protection (AMP)

Network-based *advanced malware protection* (AMP) allows the system to inspect network traffic for malware in several types of files, including PDFs, many Microsoft Office documents, and other types. When a managed device detects one of these file types, the Defense Center obtains the file's disposition and the managed device uses this information to block or allow the file.

You configure malware protection as part of your overall access control configuration; file policies associated with access control rules inspect network traffic that meets rule conditions.

Series 2 devices cannot perform network-based AMP, nor can the DC500 manage a network-based AMP deployment.

FireAMP Integration

FireAMP is an enterprise-class, advanced malware analysis and protection solution that discovers, understands, and blocks advanced malware outbreaks, advanced persistent threats, and targeted attacks.

If your organization has a FireAMP subscription, individual users install *FireAMP Connectors* on their computers and mobile devices (also called *endpoints*). These lightweight agents communicate with the Cisco cloud, which in turn communicates with the Defense Center. After you configure the Defense Center to connect to the cloud, you can use the Defense Center web interface to view endpoint-based malware events generated as a result of scans, detections, and quarantines on the endpoints in your organization.

Use the *FireAMP portal* (<http://amp.sourcefire.com/>) to configure your FireAMP deployment. The portal helps you quickly identify and quarantine malware. You can identify outbreaks when they occur, track their trajectories, understand their effects, and learn how to successfully recover. You can also use FireAMP to create custom protections, block execution of certain applications based on group policy, and create custom whitelists.

Network File Trajectory

The network file trajectory feature allows you to track a file's transmission path across a network. The system uses SHA-256 hash values to track files; so, to track a file, the system must either:

- calculate the file's SHA-256 value and perform a cloud lookup using that value
- receive endpoint-based threat and quarantine data about that file, using the Defense Center's integration with your organization's FireAMP subscription

Each file has an associated trajectory map, which contains a visual display of the file's transfers over time as well as additional information about the file.

You cannot view file trajectories for files detected by Series 2 devices, nor can you view network-based trajectories on a DC500 Defense Center.

Network Discovery

Version 5.2 integrates RNA and RUA into a feature called *discovery*, and also adds additional capabilities. Discovery can analyze IPv4 and IPv6 network traffic that is not fast-pathed at the device level, or blocked or trusted by the access control policy. In other words, only allowed traffic can be analyzed.

In the *network discovery policy*, which replaces the RNA detection policy, you can create *discovery rules* that specify exactly which network segments the system should monitor. For each segment, you can discover applications, hosts, and user activity.

Host Detection

Version 5.2 uses details unique to mobile device traffic to identify a wide variety of mobile operating systems, mobile applications, and associated mobile device hardware. The system can also detect “jailbroken” devices, that is, devices where the user has removed manufacturer limitations on the operating system.

Application Detection

Version 5.2 adds a significant number of detected applications, and introduces application control based on this detection; see [Application Control, page 1-17](#). The application management page is also redesigned and improved. For a complete list of the applications detected, see the Support Site.

User Detection

With Version 5.2, you retain the ability to perform network-based user identification using managed devices to monitor logins over IMAP, POP3, SIP/VoIP, and so on.

In conjunction with a Microsoft Active Directory deployment, you can also deploy User Agents to monitor and retrieve metadata for users as they log into the network or when they authenticate against Active Directory credentials for any other reason. Version 5.2 of the system adds the ability to perform user control for what are called *access-controlled users*; see [User Control, page 1-18](#).

Version 2.1 of the agent has flexible deployment options and includes IPv6 support. It also can detect logoffs and provide information on various types of logins, including interactive user logins to a host, remote desktop logins, file-share authentication, and computer account logins.



Note

If you want to perform user control, you **must** install and use Sourcefire User Agents. Use at least Version 2.1 of the User Agent with your Version 5.2 deployment. Support for legacy agents will be phased out in future releases. For more information, see the [Sourcefire 3D System User Agent Configuration Guide](#).

NetFlow

In Version 5.2, you continue to configure NetFlow connection logging (formerly flow data logging) in the network discovery policy. Because NetFlow data collection is not linked to access control rules, you do not have granular control over which connections you want to log. The system automatically saves all NetFlow-based connection events to the Defense Center database; NetFlow events are unidirectional and end-of-connection only.

Geolocation Information

Version 5.2's *geolocation* feature provides you with additional data about the geographical sources of routable, detected IP addresses (country, continent, and so on).

By regularly updating the geolocation database (GeoDB), you can use the Defense Center to view up-to-date granular information available for an IP address, such as postal code, coordinates, time zone, Autonomous System Number (ASN), Internet service provider (ISP), use type (home or business), organization, domain name, connection type, and proxy information. You can also pinpoint the detected location with any of four third-party map tools.

Dashboards

Version 5.2 adds predefined dashboards, as well as presets for Custom Analysis widgets and configuration options in other widgets. The changes are consistent with the added features and functionality, including: AMP, geolocation, user activity, URL tracking, and so on.

Context Explorer

Version 5.2 features the Context Explorer, which displays detailed, interactive graphical information about your monitored network, using intrusion, connection, file, geolocation, malware, and discovery data.

Distinct sections present information in the form of vivid line, bar, pie, and donut graphs, accompanied by detailed lists. You can easily create and apply custom filters to fine-tune your analysis, and you can examine data sections in more detail by clicking or hovering your cursor over graph areas.

Compared with a dashboard, which is highly customizable, compartmentalized, and updates in real time, the Context Explorer is manually updated, designed to provide broader context for its data, and has a single, consistent layout designed for active user exploration.

Reusable Objects

The system's new object manager helps you manage objects and other reusable configurations. Objects associate a name with some value or values. When you want to use that value, you can use the named object instead.

Objects can represent IP addresses or ranges of IP addresses, port-protocol combinations, VLAN tags, or URLs. You can use objects in various policies, searches, rules, and so on.

You can also use the object manager to administer:

- *application filters*, which group applications according to criteria associated with the application risk, business relevance, type, categories, and tags. You can use these filters to constrain access control rules, searches, dashboard widgets, and reports.
- the *global malware whitelist* of files (based on SHA-256 hash values) that you do not want to inspect or block using AMP; see [File Tracking, File Control, and Malware Protection, page 1-19](#).
- Security Intelligence *lists* and *feeds* of IP addresses; see [Security Intelligence Filtering, page 1-17](#).
- *security zones*, which group one or more inline, passive, switched, or routed interfaces. The interfaces in a single zone can span multiple devices; you can also configure multiple security zones on a single device. Zones allow you to manage and classify traffic flow in various policies and configurations.

Reporting

The reporting interface has been significantly redesigned to give you increased flexibility when designing *report templates* (previously *report profiles*), as well as to improve the ease of use. You can now email reports upon generation, as well as import and export report templates. You can no longer modify system-provided report templates.

The new interface also introduces the concept of report *input parameters*, which allow you to configure a report template to require the user to provide values at generation time that customize the generated report. In this way, you can dynamically tailor a report at generation time to show a particular subset of data, without changing the template.

Health Monitoring

The Defense Center now has only one default health policy, which is used as the basis for the initial health policy applied to the Defense Center, and which you can use to create your own custom health policies.

New health modules provide additional monitoring capabilities. Also, the process of blacklisting individual health modules (instead of entire appliances) is now more straightforward.

Client Vulnerabilities and VDB Updates

The system now correlates vulnerabilities with clients (previously *client applications*) running on monitored hosts, and can use those vulnerabilities to perform impact assessment. Note, however, that you cannot import third-party client vulnerabilities using the host input feature, nor can you map vendorless or versionless clients to vulnerabilities.

Also, updating the VDB on a Defense Center automatically performs the update on all its managed devices. You no longer have to explicitly update all the appliances in your deployment. Similarly, the VDB is synchronized in high-availability pairs.

User Certificates

You can now add an additional layer of authentication for client connections to the web interface. If you require user certificates, the server checks that any client browser connecting to the web server has a valid user PKI certificate, issued by the same certificate authority that issued the server certificate.

If a client's browser does not have a valid certificate, it cannot connect to the server when user certificates are enabled. You can also configure the system to check certificate revocation lists (CRLs) to identify certificates that have been revoked by the certificate authority, then ignore the invalid certificates.

IPv6 Support

You can configure the Version 5.2 management interface for IPv4-only, IPv6-only, or dual-stacked IPv4/IPv6 networks. The system can integrate with other infrastructure components and detect and process both IPv4 and IPv6 traffic. Except in a few cases, the system supports IPv6 component integration and traffic detection and processing.

For information on the unsupported and partially supported features in an IPv6 environment, please contact Support.

Application Programming Interfaces

Version 5.2 changes the way you interact with the system using a couple of the supported application programming interfaces (APIs).

Database Access

For increased security, an access list now controls which hosts can query the Defense Center's database using a third-party database access client. You can specify individual IP addresses or IP address ranges.

eStreamer

eStreamer for Version 5.2 includes many new and replaced data blocks associated with new features. Additionally, the names of some of the record and block structures and their fields have been changed to align with new terminology. There is also a new "extended" method of requesting event streams that uses a new message streaming protocol.

Although the eStreamer server continues full support of the event stream request mode used in earlier versions, to request many of the new versions of event types, you must use the extended request mode.

Depending on the type of data you stream from the system, you may need to update your eStreamer client. For detailed information, see the [Version 5.2 Sourcefire 3D System eStreamer Integration Guide](#).

Also, you can now modify your Defense Center's eStreamer configuration to stream data from an alternate management port.

Deprecated Functionality

The following sections describe the deprecated features and functionality from Version 4.10.3 to Version 5.2.

Standalone IPS Devices

Standalone devices deployed as an Intrusion detection or prevention system are no longer supported. In Version 5.2, you must manage all devices with a Defense Center.

32-Bit Virtual Appliances and Xen Hypervisor Hosting

64-bit virtual appliances running Version 5.2 are supported on the VMWare vSphere version 4.1 or 5.0 hosting environment by VMWare. Neither the Xen Hypervisor hosting environment nor 32-bit appliances are supported.

You can migrate legacy configurations and events to a new 64-bit Defense Center that you create. For information on creating a new virtual appliance, see the [Version 5.2 Sourcefire 3D System Virtual Installation Guide](#).

OPSEC

Version 5.2 does not support OPSEC integration with the intrusion policy.

Master Defense Centers

The Master Defense Center is not available with Version 5.2.

PEP

Version 5.2 integrates PEP functionality with device management (fast-path rules) and access control (PEP rules). PEP is no longer separately configurable.

Detection Engines

The system now automatically allocates its computing and detection resources. You no longer have to explicitly assign detection engines to interface sets. Most configurations and statistics that were available on a per-detection engine basis are now available on a per-device or per-interface basis, as appropriate.

Appliance Series, Models, and Capabilities

The system combines the security of an industry-leading network intrusion detection and prevention system (IPS) with the power to control access to your network based on detected applications, users, and URLs.

You can also use appliances in a switched, routed, or hybrid (switched and routed) environment; to perform network address translation (NAT); and to build secure virtual private network (VPN) tunnels among the virtual routers on managed devices, or from managed devices to remote devices.

The Defense Center provides a centralized management console and database repository. Managed devices, installed either passively or inline, on network segments monitor traffic for analysis. In addition to physical appliances, Cisco packages 64-bit virtual Defense Centers and virtual devices for the VMWare vSphere version 4.1 or 5.0 hosting environment by VMWare.

Version 5.2 is available on two series of physical appliances, as well as virtual appliances. Many capabilities are appliance dependent.

For more information, see:

- [Series 2 Appliances, page 1-25](#)
- [Series 3 Appliances, page 1-26](#)
- [Virtual Appliances, page 1-26](#)
- [Supported Capabilities by Appliance Model, page 1-26](#)

Series 2 Appliances

Version 5.2 is the first 5.x release where Series 2 appliances are supported. Series 2 is the second series of physical appliances and includes:

- 3D500, 3D1000, and 3D2000 devices
- 3D2100, 3D2500, 3D3500, and 3D4500 devices
- 3D6500 devices
- DC500, DC1000, and DC3000 Defense Centers

Series 2 devices running Version 5.2 have the same capabilities they had when running Version 4.10.3: intrusion detection and prevention (IDS/IPS), network and user discovery (RNA and RUA), and so on. They also support some new 5.x features, such as file control and basic access control.

Because of resource and architecture limitations, Series 2 devices do not support features such as Security Intelligence filtering, advanced access control, and advanced malware protection. Series 2 devices do not support any of the hardware-based features associated with Series 3 devices: switching, routing, NAT, and so on.

The DC1000 and DC3000 Defense Centers support all features; the DC500 has more limited capabilities.

Series 3 Appliances

Series 3 is the third series of physical appliances, and includes:

- 7000 Series devices
- 8000 Series devices
- DC750, DC1500, and DC3500 Defense Centers

Note that 8000 Series devices are more powerful and support a few features that 7000 Series devices do not.

Virtual Appliances

You can host 64-bit virtual Defense Centers and devices on the VMWare vSphere version 4.1 or 5.0 hosting environment by VMWare. Virtual Defense Centers can manage physical and virtual devices; physical Defense Centers can manage physical and virtual devices.

Regardless of the licenses installed and applied, virtual appliances do not support any of the system's hardware-based features: redundancy (high availability, stacking, clustering), switching, routing, and so on. Also, virtual devices do not have web interfaces.

32-bit virtual appliances and Xen Hypervisor hosting environments are not supported with Version 5.2. You can, however, migrate configurations from your existing 32-bit Version 4.10.3 virtual appliances to a newly created 64-bit Version 5.2 Defense Center.

Supported Capabilities by Appliance Model

Many capabilities are appliance and license dependent. The following table matches the major capabilities of the system with the appliances that support those capabilities, assuming you have the correct licenses installed and applied.



Tip

For information on the terms used in the table, see: [New and Changed Terminology, page 1-2](#) and [New, Changed, and Updated Features and Functionality, page 1-3](#). You can also find detailed information in the [Version 5.2 Sourcefire 3D System User Guide](#).

Keep in mind that in Version 5.x, analysis functions are restricted to the Defense Center. Only essential management and monitoring functions are available on managed devices; standalone device deployments are not supported. In the table, the Defense Center column for device-based capabilities (such as stacking, switching, and routing) indicates whether that Defense Center can manage and configure devices to perform their functions. For example, you can use a Series 2 DC1000 to manage NAT on Series 3 devices. Also note that certain Defense Center-based features, such as high availability and FireAMP integration, are not relevant to managed devices.

Table 1-4 Supported Capabilities by Appliance Model

| Feature | Series 2 Device | Series 2 Defense Center | Series 3 Device | Series 3 Defense Center | Virtual Device | Virtual Defense Center |
|--|-----------------|-------------------------|-------------------------------|-------------------------|----------------|------------------------|
| network discovery: host, application, and user | yes | yes | yes | yes | yes | yes |
| geolocation data | yes | DC1000, DC3000 only | yes | yes | yes | yes |
| intrusion detection and prevention (IPS) | yes | yes | yes | yes | yes | yes |
| Security Intelligence filtering | no | DC1000, DC3000 only | yes | yes | yes | yes |
| access control: basic network control | yes | yes | yes | yes | yes | yes |
| access control: applications | no | yes | yes | yes | yes | yes |
| access control: users | no | DC1000, DC3000 only | yes | yes | yes | yes |
| access control: literal URLs | no | yes | yes | yes | yes | yes |
| access control: URL filtering by category and reputation | no | DC1000, DC3000 only | yes | yes | yes | yes |
| file control: by file type | yes | yes | yes | yes | yes | yes |
| network-based advanced malware protection (AMP) | no | DC1000, DC3000 only | yes | yes | yes | yes |
| FireAMP integration | no | yes | no | yes | no | yes |
| fast-path rules | no | yes | 8000 Series only | yes | no | yes |
| strict TCP enforcement | no | yes | yes | yes | no | yes |
| configurable bypass interfaces | yes | yes | except where hardware limited | yes | no | yes |
| tap mode | no | yes | yes | yes | no | yes |
| switching and routing | no | yes | yes | yes | no | yes |
| NAT policies | no | yes | yes | yes | no | yes |
| VPN | no | yes | yes | yes | no | yes |
| high availability | no | DC1000, DC3000 only | no | DC1500, DC3500 only | no | no |
| device stacking | no | yes | 3D8140, 82xx Family only | yes | no | yes |

Table 1-4 Supported Capabilities by Appliance Model (continued)

| Feature | Series 2 Device | Series 2 Defense Center | Series 3 Device | Series 3 Defense Center | Virtual Device | Virtual Defense Center |
|-------------------|-----------------|-------------------------|--------------------------|-------------------------|----------------|------------------------|
| device clustering | no | yes | yes | yes | no | yes |
| clustered stacks | no | yes | 3D8140, 82xx Family only | yes | no | yes |
| interactive CLI | no | no | yes | no | yes | no |

Where Do I Begin?

The chapters in this guide step you through the process of migrating vital configurations and events from either a Version 4.10.3 Defense Center or standalone 3D Sensor to a Version 5.2 Defense Center. To migrate your deployment, read and follow the directions in these chapters.

Understanding the Migration Process

[Understanding the Migration Process, page 2-1](#) provides an overview of the migration process. This chapter explains the importance of planning your migration and the advantages and limitations of reimaging your existing Version 4.10.3 appliances or deploying new Version 5.2 appliances.

Example scenarios are designed to help you develop a plan for migrating your unique deployment:

- migrating a multi-sensor deployment with either a replacement or a reimaged Defense Center, or a re-created virtual Defense Center
- performing a “rolling” migration where you replace sensors in turn to minimize inspection downtime
- migrating stacked 3D Sensors
- migrating a deployment with a high availability Defense Center pair
- migrating standalone 3D Sensors with IPS

Preparing for Migration

[Preparing for Migration, page 3-1](#) helps you prepare to migrate your deployment from Version 4.10.3 to Version 5.2 smoothly and without error. Read this chapter to make sure you understand:

- the appliance models that you can migrate, including licensing requirements, and the capabilities of your deployment after you install Version 5.2
- system software and intrusion rule update requirements
- for virtual appliances, host environment and memory requirements
- how the migration affects your organization’s network traffic
- when and how to perform the migration so as to least disrupt your deployment
- the consequences of and how to avoid configurations that translate poorly to the Version 5.2 architecture
- how to obtain, identify, and install the migration scripts

Performing the Migration

[Performing the Migration, page 4-1](#) steps you through the actual migration process, which is done by running system-provided scripts using an appliance's shell according to your migration plan. For your convenience, the chapter also describes steps you must take after you run the scripts, using the Version 5.2 Defense Center web interface.

Understanding Migrated Configurations and Events

[Understanding Migrated Configurations and Events, page 5-1](#) helps you understand exactly:

- which configurations and events will be migrated
- which configurations have changed location or names due to terminology changes and the redesigned web interface
- what new configurations will be created on the Version 5.2 Defense Center

The chapter also helps you understand what will not be migrated, and therefore which configurations you must re-create.

For More Information

For more information on how you can upgrade to newer versions of the Sourcefire 3D System, now known as the FireSIGHT System, refer to the documentation resources listed in the [FireSIGHT System Documentation Roadmap](#).



Understanding the Migration Process

Cisco provides scripts that allow you to migrate vital configurations and events to a Version 5.2 Defense Center from either a Version 4.10.3.x Defense Center or standalone 3D Sensors with IPS. Additionally, you can run a sensor migration script from your Version 5.2.0.x Defense Center to remotely reimage one or more Series 2 and Series 3 sensors in parallel from Version 4.10.3 (or a later patch) to Version 5.2.

The migration process you design for your deployment will be unique and will depend on multiple factors, including (but not limited to) the models of your appliances and your physical access to them, whether you have spare or replacement appliances to use, the number and complexity of configurations you want to migrate, whether you want to migrate events, and so on.

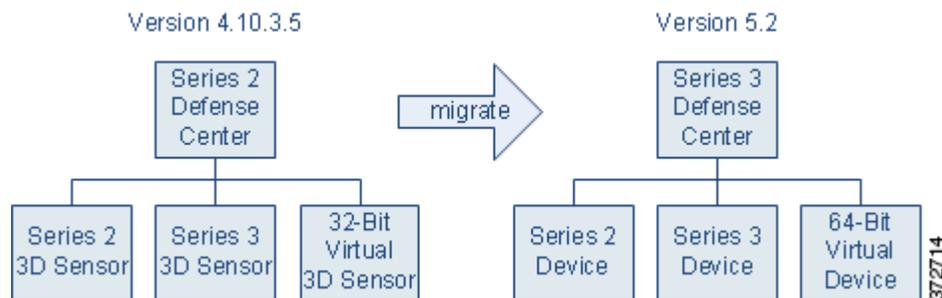
Before you begin to migrate any deployment, thoroughly read this guide and understand the requirements, steps involved, and expected results of the migration. Then, create a detailed plan tailored to your organization.



Note

Before you begin the migration process you **must** make sure you have a detailed plan and that you have fully prepared your appliances, including obtaining and installing the new licenses, resolving issues that could prevent a clean migration, setting up replacement appliances, installing the migration utilities, and so on. For detailed information, see [Preparing for Migration, page 3-1](#).

To help you understand the basic migration process, this chapter presents a scenario where you migrate a simple deployment of a Defense Center managing three 3D Sensors from Version 4.10.3 to Version 5.2, while also replacing the Defense Center.



Tip

For simplicity, examples use individual managed sensors. However, you can also simultaneously replace or reimage groups of sensors.

Note that this scenario retains all of the physical devices in the deployment, choosing to reimage them to Version 5.2. This is cost effective, but you lose the inspection capabilities of each Series 2 and Series 3 sensor while they are being reimaged to Version 5.2. Additionally, reimaging an inline sensor without the sensor migration script, or with the script when the sensor is not configured to fail open, causes the sensor to fail closed until it is registered to a Version 5.2 Defense Center and its interfaces are reconfigured. In these cases, you may want to disconnect inline sensors from your critical network path during the reimage and configuration portion of the migration process.

There are, however, alternatives, including replacing one or more devices. One-for-one replacements minimize inspection downtime because you can set up a parallel Version 5.2 deployment, migrate configurations, then simply switch cabling over when you are ready. However, this can be costly and requires careful planning to make sure you have the licenses, resources, and physical access to deploy multiple replacement appliances.

With at least one spare device, there is a compromise: a “rolling” migration that replaces each sensor in turn: use the replacement Defense Center to apply equivalent configurations from a Version 4.10.3 sensor to a replacement Version 5.2 device, switch cabling over from sensor to device, then reimage the now-disconnected sensor to Version 5.2 to act as the replacement device for the next Version 4.10.3 sensor. This type of rolling migration minimizes inspection downtime, because for each sensor-to-device migration you only need to interrupt traffic for the recabling. However, this scenario also requires extended physical access and moving of appliances.

Keep the alternatives in mind as you plan your migration. The following sections give you an overview of the migration process for the basic scenario shown above, and describe common variations that may apply to your deployment:

- [CAUTION: Do Not Interrupt the Reimage Process, page 2-2](#)
- [Migrating a Simple Multi-Sensor Deployment, page 2-3](#)
- [Performing a Multi-Sensor Rolling Migration, page 2-11](#)
- [Migrating Stacked 3D Sensors, page 2-13](#)
- [Migrating By Reimaging the Existing Defense Center, page 2-14](#)
- [Migrating a Deployment with a Virtual Defense Center, page 2-24](#)
- [Migrating High Availability Defense Center Pairs, page 2-25](#)
- [Migrating Standalone 3D Sensors with IPS, page 2-27](#)



Tip

This chapter provides an overview of the migration process to help you plan, but does not go into detail about the steps involved. For detailed information on those steps, see the next chapters: [Preparing for Migration, page 3-1](#) and [4, page 4-1](#).

CAUTION: Do Not Interrupt the Reimage Process

Supported Devices: Any

Supported Defense Centers: Series 2, Series 3

When your migration involves reimaging (a process that is also commonly referred to as *restoring*) a Defense Center or sensor from Version 4.10.3 to Version 5.2, you must allow time for the process to complete. Interrupting the process can result in an unrecoverable error.

You reimage a Defense Center using the same basic process that you would use to reimage from one version to another. There is no special reimage process for Defense Centers.

Version 5.2 managed devices were more commonly referred to as *sensors* with Version 4.10.x. You can reimage managed devices either manually or using a sensor migration script.

Defense Centers and Managed Devices: Manual Reimage

The time required to reimage a Defense Center, or a sensor when you do not use the sensor migration script, depends on the model. It is reasonable to assume that the minimum time for reimagining a Defense Center would be at least 45 minutes. There is no specific data giving an average or minimum time when you reimage a managed device and do not use the migration script.

Interrupting the reimage process for either - by pressing Ctrl + C, rebooting, or otherwise - can result in an unrecoverable error. Contact Support if you experience any issue with the process. It is imperative that you do not quit, reboot, or otherwise interrupt the process.

Managed Devices: Migration Script Reimage

It is imperative that you not interrupt the reimage process while reimagining a managed device using the migration script. This includes not stopping the Defense Center where you run the script, by rebooting or otherwise. Contact Support if you experience any issue with the process.

You can use Ctrl + C to stop the migration script before the reimage starts. However, the script disables Ctrl + C when you have entered all commands and the reimage begins.

The following table provides average times by model encountered when reimagining either in a single location or in different locations with large bandwidth connections between locations.

Table 2-1 Average Managed Device Reimage Times in Favorable Environments

| Device | Time |
|------------------------------|-------------------|
| 3D1000 | 1 hour 40 minutes |
| 3D2000 | 1 hour 40 minutes |
| 3D2500 | 1 hour 28 minutes |
| 3D3500 | 1 hour 28 minutes |
| 3D4500 | 1 hour 25 minutes |
| 3D6500 | 1 hour 25 minutes |
| 3D7030 | 1 hour 35 minutes |
| 3D500 | 2 hours 5 minutes |
| 3D7110 | 1 hour 35 minutes |
| 3D7120 | 1 hour 35 minutes |
| Series 3 (3D8140, 3D8250) | 1 hour 35 minutes |

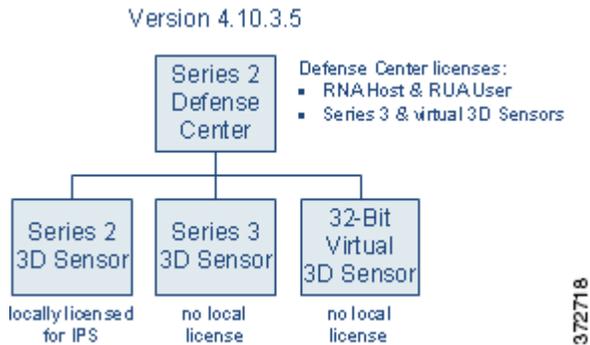
Connection bandwidth can have a significant impact on reimage time, and must be considered so you can anticipate issues. Contact Support before reimagining if you are not sure that you can complete the process without interrupting it.

Migrating a Simple Multi-Sensor Deployment

Supported Devices: Any

Supported Defense Centers: Series 2, Series 3

Although every organization is unique, to help you understand the basic migration process, consider the following simple Version 4.10.3 deployment.



In this deployment, a Series 2 Defense Center manages three 3D Sensors deployed inline: a Series 2 sensor, a Series 3 sensor, and a 32-bit virtual sensor.

So all the sensors can collect both network (RNA) and user (RUA) data, as well as act as an intrusion prevention system (IPS), this deployment includes the following licenses:

- RNA Host and RUA User feature licenses installed on the Defense Center
- licenses for the Series 3 and virtual sensors, also installed on the Defense Center
- a local IPS license installed on the Series 2 sensor

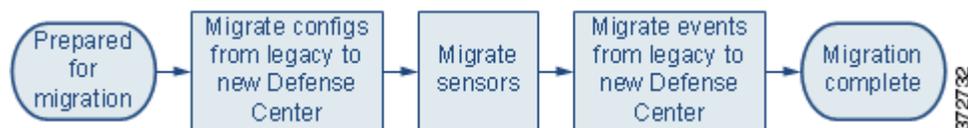
Now, you want to migrate your deployment to Version 5.2. In this scenario, you are replacing the Series 2 Defense Center with a Series 3 Defense Center, but are not replacing the physical sensors. Instead, you will reimage those sensors to Version 5.2. You must replace the virtual device; Version 5.2 supports only 64-bit virtual appliances.

**Tip**

When you replace an appliance, consider your current and future performance needs. For assistance, contact Sales.

Cisco recommends that you replace your Defense Center for ease of migration and to minimize downtime. If you are not replacing your existing Defense Center; see [Migrating By Reimaging the Existing Defense Center, page 2-14](#).

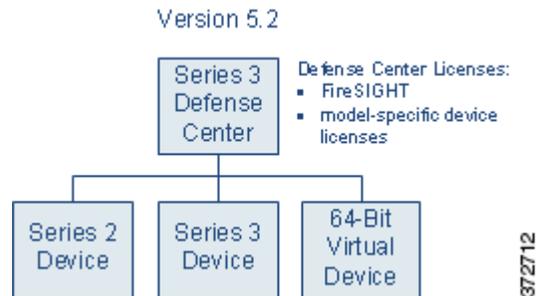
With a replacement, both Defense Centers running at the same time means that you can first copy configuration and event packages directly from Defense Center to Defense Center, then migrate the devices from one active deployment to another. Finally, if you want to migrate events, you can do it at the end of the process when it causes the least disruption.

**Caution**

Always migrate configurations before events. Migrating events before configurations can result in unpredictable event display and behavior.

Note that you do not need to export any configurations or events from the sensors; these are migrated as part of the Defense Center process.

When this migration is complete, a new Series 3 Defense Center will manage three devices deployed inline: your reimaged Series 2 device, your reimaged Series 3 device, and a newly created 64-bit virtual device.



In Version 5.2, which uses a different licensing scheme than Version 4.10.3, you use the Defense Center to control licenses for itself and the devices it manages, and devices are never licensed locally. So that this migrated deployment can behave equivalently with your Version 4.10.3 deployment, you must install the following licenses on the Version 5.2 Defense Center:

- a FireSIGHT license, which replaces the RNA Host and RUA User licenses
If you reimage the Defense Center instead of replacing it, you may be able to use your legacy licenses; see [Host and User Licenses, page 1-4](#).
- model-specific Protection licenses for both the Series 3 and the virtual devices

You do not need a license for the Series 2 device; these devices automatically have most Protection capabilities. However, you do need a Threat & App (TA) subscription.

After you have fully prepared, you can begin the migration process, which has the following phases:

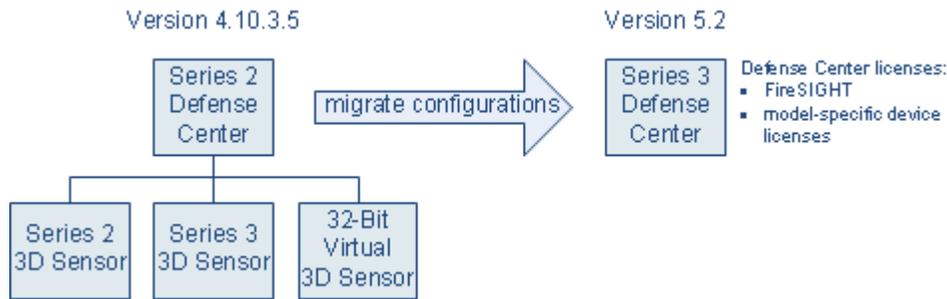
- [Migrating Configurations to a Replacement Defense Center, page 2-5](#)
- [Migrating 3D Sensors, page 2-6](#)
- [Migrating Events from Defense Center to Defense Center, page 2-10](#)

Migrating Configurations to a Replacement Defense Center

Supported Defense Centers: Series 2, Series 3

In this scenario, the Version 4.10.3 Series 2 Defense Center is replaced with a new Version 5.2 Series 3 Defense Center. If you do not have a replacement and must reimage your existing Defense Center, export legacy events before you reimage if you want to retain them; see [Migrating By Reimaging the Existing Defense Center, page 2-14](#).

After you finish this phase, your Version 4.10.3 configurations are imported onto the Version 5.2 Defense Center. However, the Version 4.10.3 deployment is still intact and operating normally.



To migrate configurations between Defense Centers:

Access: Admin

- Step 1** On the Version 4.10.3 Defense Center, run the configuration export script to create a package of supported configurations; see [Exporting Configurations from a Version 4.10.3 Appliance, page 4-3](#). The export script analyzes the configurations and lists those that cannot be migrated (cleanly or otherwise) to Version 5.2.



Note Cisco recommends exiting the script to resolve any issues with configurations essential to your deployment. If you continue without resolving the issues, some configurations will not be migrated, though you may be able to resolve specific issues during the import process. For more information, see [Addressing Configuration Incompatibilities, page 3-7](#).

- Step 2** Copy the export package to the Version 5.2 Defense Center.
- Step 3** On the Version 5.2 Defense Center, run the configuration import script to import the configurations in the package; see [Importing Configurations onto a Version 5.2 Defense Center, page 4-7](#). The import script analyzes the configurations and, like the export script, lists those that cannot be migrated. It also gives you the opportunity to resolve any correctable issues with the imported configurations, such as detection engine-specific settings that do not migrate cleanly to Version 5.2. You also must specify some basic information for your Version 5.2 deployment, such as security zones and basic access control settings.
- Step 4** Verify the successful migration of your configurations. For information on what to expect from migrated and new configurations, see [Understanding Migrated Configurations and Events, page 5-1](#).
- Step 5** To migrate your sensors to the Version 5.2 Defense Center, continue with the next section, [Migrating 3D Sensors](#).

Migrating 3D Sensors

Supported Devices: Any

Because Version 5.2 Defense Centers cannot manage Version 4.10.3 3D Sensors, after you migrate the Defense Center, you must update the devices it will manage. Because there is no direct update process, you must replace or reimage your 3D Sensors.

When migrating a physical 3D Sensor, you can use your existing appliance (reimage) or you can replace it. In this scenario, we are reusing both the Series 2 and Series 3 devices, and do not have a spare. You must replace the virtual device; Version 5.2 supports only 64-bit virtual appliances.

You do not need to migrate any configurations or events between sensors. You simply use the sensor migration script to update the software on the sensor. The script copies the sensors' interface configurations, reimages the sensors, registers them to the Defense Center, and applies the interface configurations. If you do not use the script, you must complete these tasks manually. Regardless of whether you use the sensor migration script, you must manually apply the configurations imported by the configuration import script.

For more information, see:

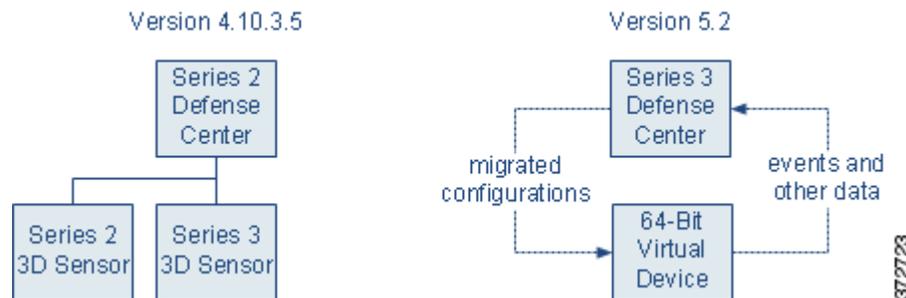
- [Migrating Virtual Sensors by Replacement, page 2-7](#)
- [Migrating Series 2 and Series 3 Sensors by Reimage, page 2-8](#)

Migrating Virtual Sensors by Replacement

Supported Devices: virtual

Migrating virtual 3D Sensors is straightforward: because there is no hardware to reimage; you simply create a replacement virtual device, register it to the new Defense Center, and apply migrated configurations to it.

At that point, the new device is handling network traffic and reporting events to the Version 5.2 Defense Center. The physical Version 4.10.3 sensors are still handling their own network traffic, and are still reporting to the Version 4.10.3 Defense Center.



To replace a virtual sensor:

Access: Admin

Step 1 Create a new 64-bit virtual device using the VMware vSphere Client. Use the device's CLI to perform its initial setup, including registration (that is, specifying your new Version 5.2 Defense Center as its manager).

Version 5.2 packages 64-bit virtual appliances only for the VMware ESX/ESXi hosting environment. For more information on the requirements for the hypervisor host, as well as information on creating and setting up virtual appliances, see the [Version 5.2 Sourcefire 3D System Virtual Installation Guide](#).

Step 2 Using its hypervisor host, remove the inline Version 4.10.3 virtual device from the network path so that traffic can continue to flow while you bring up the replacement device.

For more information, see the documentation for the hypervisor host you are using to run Version 4.10.3 virtual appliances.

Step 3 Using the Version 4.10.3 Defense Center's web interface, remove the device from management.



Tip

After you remove the Version 4.10.3 device from your deployment, uninstall it to free resources on your 32-bit hypervisor host.

Step 4 Use the Version 5.2 Defense Center's web interface to add and configure the Version 5.2 device, including applying a license, adding its interfaces to zones, and applying the policies created and updated by the migration.

For more information, see [Completing Your Version 5.2 Deployment, page 4-33](#).

Step 5 Using the VMware vSphere Client on your 64-bit hypervisor host, place the new Version 5.2 device inline.

Step 6 Continue with the next section, [Migrating Series 2 and Series 3 Sensors by Reimage](#), to migrate your physical sensors to the Version 5.2 Defense Center.

Migrating Series 2 and Series 3 Sensors by Reimage

Supported Devices: Series 2, Series 3

When migrating a physical 3D Sensor, you can use your existing appliance (reimage) or you can replace it. In this scenario, we are reusing both physical sensors, and do not have a spare.



Tip

If you have spare sensors, you can perform one-for-one replacements or plan a rolling migration that swaps out each sensor in turn. These strategies can minimize downtime but may not be practical given the size of your deployment and physical access to the sensors; see [Performing a Multi-Sensor Rolling Migration, page 2-11](#).

To use an existing sensor, you must reimage it to Version 5.2 and apply migrated configurations to it. If you do not use the sensor migration script, you must manually register the sensor before applying configurations.

Reimaging results in the loss of almost all configuration and event data on the sensor. Reimaging can retain the sensor's network, console, and Series 3 Lights-Out Management (LOM) settings, and the sensor migration script registers sensors and preserves interface configurations. However, you must perform all other setup tasks after the restore process completes.

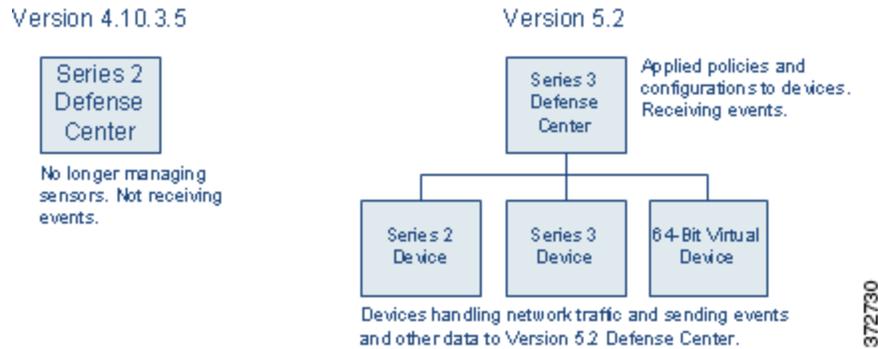


Note

Inline interfaces **fail closed** during the reimage when you do not use the sensor migration script or you use the script and the interfaces are not configured to fail open. In these cases you may want to remove the sensors from your critical network path during reimage, which may require physical access to the sensors.

When you do not use the sensor migration script, physical access is required to reimage Series 2 sensors, even those deployed passively; the standard Series 2 restore utility is distributed on an external USB drive. Also, when you do not use the sensor migration script, you can remotely reimage Series 3 sensors using either a remote KVM or, if enabled, LOM.

After you migrate your Version 4.10.3 sensors to Version 5.2 managed devices, the reimaged devices are handling network traffic and reporting events to the Version 5.2 Defense Center. The Version 4.10.3 Defense Center is no longer managing any sensors or receiving new events. However, it may have stored events that you want to view, so leave it powered on and connected to the management network for now.



To migrate a Series 2 or Series 3 3D Sensor using the sensor migration script:

Access: Admin

-
- Step 1** If any Version 4.10.3 Series 2 or Series 3 inline sensor will be configured to fail closed when you reimagine it, remove it from the network path so that traffic can continue to flow while you reimagine it.
- Step 2** On the Defense Center, run the sensor migration script to reimagine your physical sensors; see [Reimaging and Registering Devices with the Sensor Migration Script](#), page 4-22.
- The script copies the Series 2 and Series 3 interface configurations, reimages the sensors, registers the reimaged sensors to the Defense Center, and applies the interface configurations. For more information, see [Reimaging and Registering Devices with the Sensor Migration Script](#), page 4-22.
- Step 3** Use the Version 5.2 Defense Center's web interface to configure each device, including applying a license, adding its interfaces to zones, and applying the policies created and updated by the migration.
- For more information, see [Completing Your Version 5.2 Deployment](#), page 4-33.
- Step 4** If you previously removed any inline sensors that were configured to fail closed from the network path prior to reimaging them, place the freshly set up Version 5.2 devices inline.
- Step 5** Continue with the next section, [Migrating Events from Defense Center to Defense Center](#), to migrate legacy events.
-

To migrate a Series 2 or Series 3 3D Sensor manually:

Access: Admin

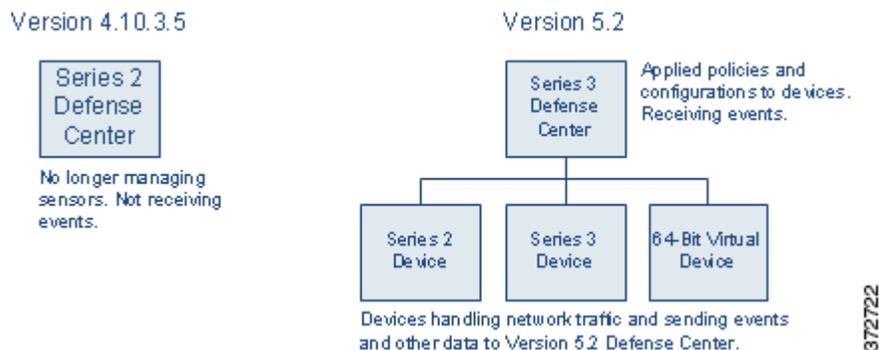
-
- Step 1** Remove either inline Version 4.10.3 sensor from the network path so that traffic can continue to flow while you reimagine it.
- Whether you reimagine your sensors at once or serially depends on your migration plan. In this case, we are reimaging one sensor after the other.
- Step 2** Using the Version 4.10.3 Defense Center's web interface (**Operations > Sensors**), remove the sensor from management.

- Step 3** Reimage the Version 4.10.3 sensor to a Version 5.2 device and perform the initial setup on the device. For more information, see the [Version 5.2 Sourcefire 3D System Installation Guide](#).
- Step 4** Use the Version 5.2 Defense Center's web interface to add and configure the device, including applying a license, adding its interfaces to zones, and applying the policies created and updated by the migration. For more information, see [Completing Your Version 5.2 Deployment](#), page 4-33.
- Step 5** Place the freshly set up Version 5.2 device inline.
- Step 6** Repeat this procedure for the other physical sensor.
- Step 7** Continue with the next section, [Migrating Events from Defense Center to Defense Center](#), to migrate legacy events.

Migrating Events from Defense Center to Defense Center

Supported Defense Centers: Any

This scenario includes the optional migration of legacy intrusion and audit events from the Version 4.10.3 Defense Center to the Version 5.2 Defense Center. If you replaced your Defense Center as in this scenario, it is no longer managing any sensors or receiving new events, but you can migrate stored events to the Version 5.2 Defense Center.



If you are not interested in events generated before the migration, you can skip this step.



Note

If you are reimagining your existing Defense Center to Version 5.2 and want to migrate legacy events, you must perform this step **before** you reimage the appliance and migrate the sensors. For more information, see [Migrating By Reimagining the Existing Defense Center](#), page 2-14.

Note that the fields in intrusion events generated by Version 4.10.3 are different than the fields in Version 5.2 intrusion events. For information on how legacy events appear in the Version 5.2 web interface, see [Understanding Migrated Intrusion and Audit Events](#), page 5-18.

Also keep in mind that when you migrate events, the timestamps on those events will be “behind” newly generated events on the Version 5.2 Defense Center. Because the database is pruned by event timestamp, your migrated events will be pruned before those events.

After you migrate events, you can shut down and remove the Version 4.10.3 Defense Center from your deployment (or, if you are reusing the Defense Center, reimage it to Version 5.2).

To migrate events between Defense Centers:**Access:** Admin

-
- Step 1** On the Version 4.10.3 Defense Center, run the event export script to create a package of intrusion and audit events; see [Exporting Events from a Version 4.10.3 Appliance, page 4-6](#).
- Step 2** Copy the event package to the Version 5.2 Defense Center.
- Step 3** On the Version 5.2 Defense Center, run the import events script to import the events in the package; see [Importing Events onto a Version 5.2 Defense Center, page 4-20](#).

The script analyzes the package and displays the disk space required to import the events. You can abort the import if the events require too much space. Otherwise, continue to import the events.

Performing a Multi-Sensor Rolling Migration

Supported Devices: Series 2, Series 3

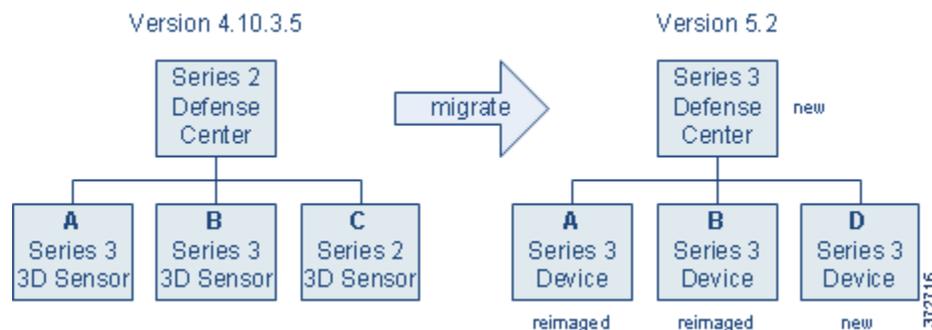
A “rolling” migration from Version 4.10.3 to Version 5.2 replaces each sensor in a deployment in turn to minimize inspection downtime. The basic strategy is to use a replacement Defense Center to apply equivalent configurations from a Version 4.10.3 sensor to a replacement Version 5.2 device, switch cabling over from sensor to device, then reimage the now-disconnected sensor to Version 5.2 to act as the replacement device for the next Version 4.10.3 sensor.

This means that for each sensor-to-device migration you only need to interrupt traffic flow for the recabling. However, this scenario also requires extended physical access to and moving of appliances, as well as a replacement physical or virtual Defense Center.

**Note**

If you are reimaging your existing Defense Center, there is no advantage to a rolling migration. See [Migrating By Reimaging the Existing Defense Center, page 2-14](#).

Now, consider a scenario similar to that in [Migrating a Simple Multi-Sensor Deployment, page 2-3](#), except in this case the Version 4.10.3 Defense Center is managing two Series 3 sensors (A and B) and one Series 2 (C). When you migrate this deployment to Version 5.2, you want to replace both the Defense Center and the Series 2 sensor with Series 3 appliances.



Preparing for this migration includes fully setting up the Version 5.2 replacement Defense Center as well as the new Series 3 device (D) that will replace your Series 2 sensor. Then, you can migrate configurations from Defense Center to Defense Center, as described in [Migrating Configurations to a](#)

[Replacement Defense Center, page 2-5.](#)

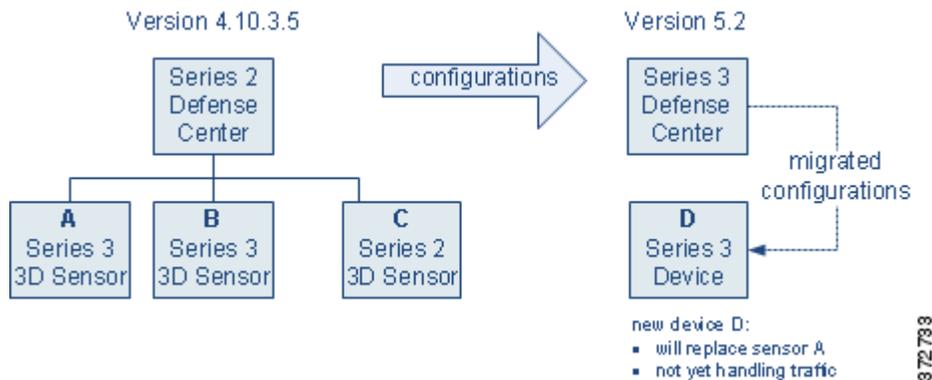
After the replacement Defense Center has the configurations it needs to manage your migrated deployment, you can use the Defense Center to add and configure the new device D as described in [Completing Your Version 5.2 Deployment, page 4-33](#). Make sure you enable a Protection license, apply the access control policy created by the migration, and apply a device configuration that adds the device's interfaces to the appropriate zones (also created by the migration).



Note

Add interfaces to zones based on which Version 4.10.3 sensor you are replacing right now. In this example, where you are replacing sensor A with device D, assign the interfaces on D to the zones that represent network traffic monitored by the interfaces on A. For a detailed explanation, see [Configuring and Verifying Sensing Interfaces and Inline Sets, page 4-33](#).

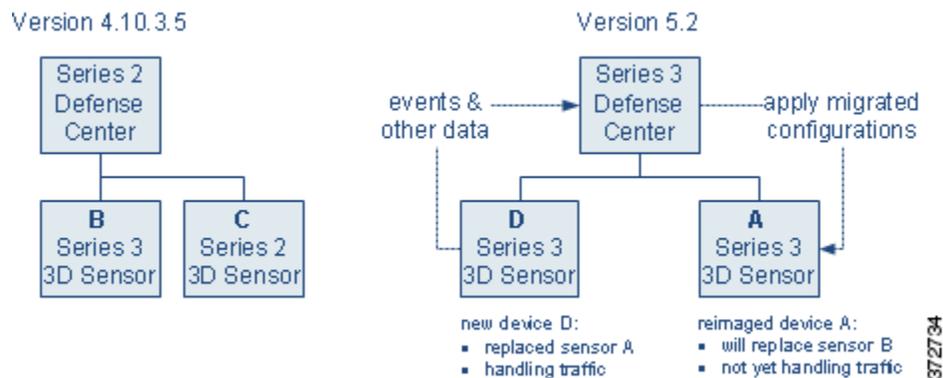
At this point, the Version 4.10.3 deployment is still intact. The Version 5.2 replacement Defense Center is managing replacement device D, which is ready to be placed inline and take over for sensor A.



Now, you can switch the cabling from sensor A to device D to have your Version 5.2 deployment begin handling network traffic previously inspected by sensor A.

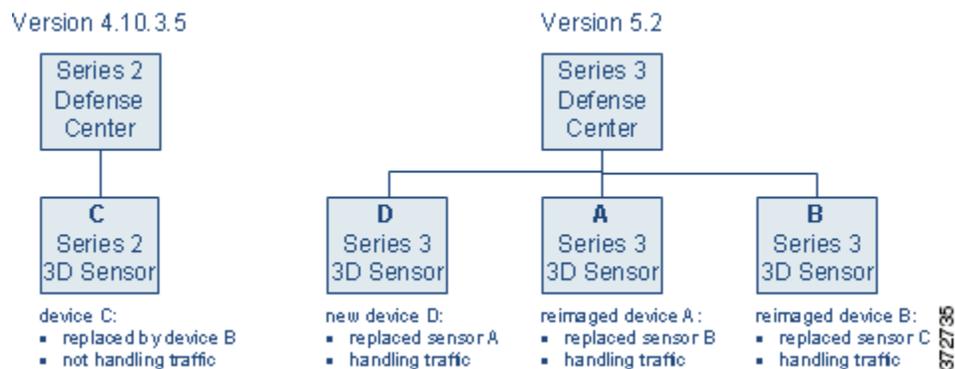
You now have a new spare sensor, A, and can repeat the process. Use the Version 4.10.3 Defense Center to delete sensor A from management, reimage it to Version 5.2, and add it to the Version 5.2 Defense Center as a replacement for the next sensor to be migrated: B. Optionally, you can use the sensor migration script to reimage sensor A and register it to the Version 5.2 Defense Center. As before, enable a Protection license, apply a device configuration that adds the device's interfaces to the appropriate zones, and apply the access control policy created by the migration.

At this point, the Version 4.10.3 deployment includes sensors B and C. The Version 5.2 sensor D has taken over for Version 4.10.3 sensor A, which has been reimaged to Version 5.2 and is ready to take over for sensor B.



Now, you can switch the cabling from sensor B to reimaged device A to have your Version 5.2 deployment begin handling network traffic previously inspected by sensor B. Your spare sensor is now sensor B, which you can use to replace sensor C.

After you replace sensor C, your Version 5.2 deployment has fully replaced your Version 4.10.3 deployment.



The Version 4.10.3 Defense Center is now managing only sensor C, which is not inspecting any traffic. You can power down and disconnect the sensor. However, If the Defense Center has stored events that you want to migrate, leave it powered on and connected to the management network until you perform the steps in [Migrating Events from Defense Center to Defense Center](#), page 2-10.

Migrating Stacked 3D Sensors

Supported Devices: 8000 Series

When you reimage a 3D Sensor, you lose almost all configuration and event data on the appliance, including stacking configurations. Because reimaging a sensor automatically breaks the stack, migrating stacked sensors is not significantly different from migrating single sensors.

If your Version 4.10.3 deployment includes stacked sensors, first delete the stack from the managing Version 4.10.3 Defense Center, then reimage the stacked sensors. Re-establish the stack after adding the devices to the Version 5.2 Defense Center.



Note

You must obtain a model-specific Protection license for each Series 3 device you plan to stack.

Migrating By Reimaging the Existing Defense Center

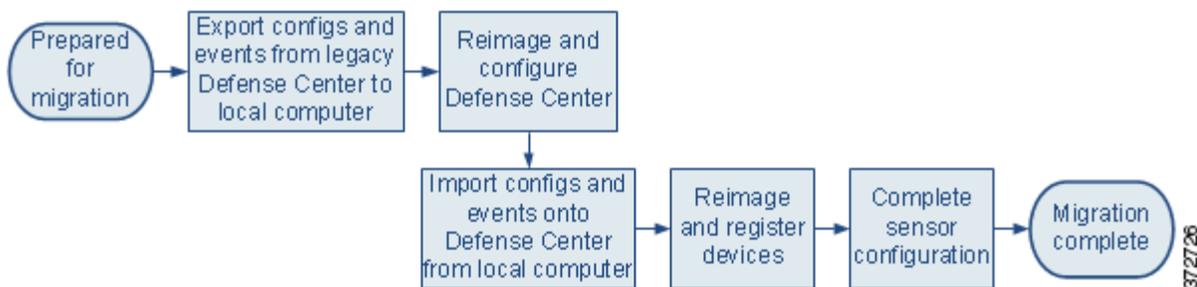
Supported Devices: migration method dependent

Supported Defense Centers: Series 2, Series 3

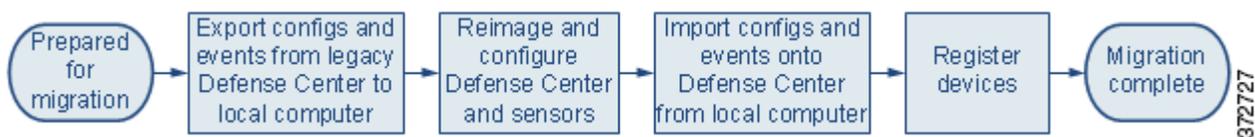
In the simple scenario presented earlier in this chapter (see [Migrating a Simple Multi-Sensor Deployment, page 2-3](#)), you replaced the Series 2 Defense Center in your deployment with a Series 3 Defense Center running Version 5.2. Replacing the Defense Center is convenient and can minimize downtime, but if you do not have the resources to replace the Defense Center, you must reimage your existing Defense Center to Version 5.2.

In this reimage scenario, when you export configurations and events from the Version 4.10.3 Defense Center you must copy them to a local computer so they are not lost while you reimage and reconfigure your appliances. After you reimage the Defense Center, you must set it up and prepare it for migration, then import the configurations and events and, finally, if you do not use the sensor migration script, re-register the migrated sensors, configure sensor interfaces, and apply the interface configurations.

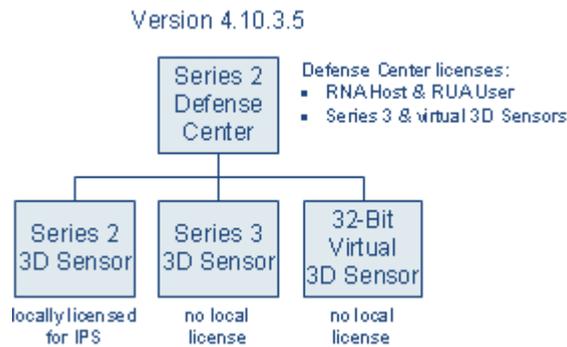
Whether you use the sensor migration script depends on your migration plan. The migration scenario in the following diagram assumes that you use the sensor migration script. When you use the script, Cisco recommends that you reimage devices **after** reimaging the Defense Center and importing configurations, so policies are in place and ready to apply.



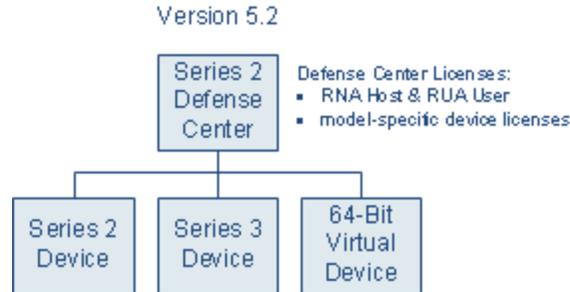
The following diagram shows an alternative migration sequence where you do **not** use the sensor migration script. In this case, you might find it convenient to reimage your sensors and the Defense Center before importing configurations, but you should register your devices after importing configurations and events so your configurations and events are in place.



Once again, consider the following simple Version 4.10.3 deployment, where a Series 2 Defense Center manages three 3D Sensors deployed inline: a Series 2 sensor, a Series 3 sensor, and a 32-bit virtual sensor:



Now, you want to migrate your deployment to Version 5.2 **without** replacing any of the physical appliances. In your Version 5.2 deployment, a reimaged Series 2 Defense Center will manage three devices deployed inline: your reimaged Series 2 device, your reimaged Series 3 device, and a newly created 64-bit virtual device.



So that this migrated deployment can behave equivalently with your Version 4.10.3 deployment, install the following licenses on the reimaged Version 5.2 Defense Center:

- your RNA Host and RUA User licenses from Version 4.10.3

These legacy licenses function identically to the newer FireSIGHT license. You can obtain a FireSIGHT license for your reimaged Defense Center, but it is not required. For more information, see [Host and User Licenses, page 1-4](#).

- model-specific Protection licenses for both the Series 3 and the virtual devices

You do not need a license for the Series 2 device; these devices automatically have most Protection capabilities. However, you do need a Threat & App (TA) subscription.

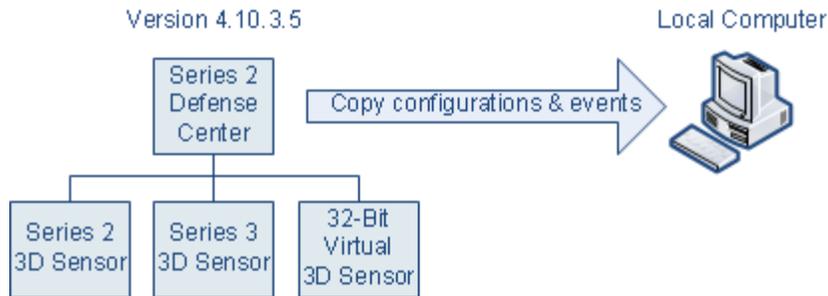
For more information on the phases in this migration process, see:

- [Exporting Configurations and Events from the Defense Center, page 2-15](#)
- [Completing the Migration Using the Sensor Migration Script, page 2-16](#)
- [Completing the Migration Manually, page 2-21](#)

Exporting Configurations and Events from the Defense Center

Supported Defense Centers: Series 2, Series 3

After you fully prepare for migration, the first step when migrating a deployment where you are going to reimage the Defense Center is to create configuration and export packages on the Version 4.10.3 Defense Center, then copy them to a local computer.



To export configurations and events from a Defense Center you are going to reimage:

Access: Admin

Step 1 On the Defense Center, run a configuration export script to create a package of supported configurations; see [Exporting Configurations from a Version 4.10.3 Appliance, page 4-3](#).

The export script analyzes the configurations and lists those that cannot be migrated (cleanly or otherwise) to Version 5.2.



Note Cisco recommends exiting the script to resolve any issues with configurations essential to your deployment. If you continue without resolving the issues, some configurations will not be migrated, though you may be able to resolve specific issues during the import process. This is especially important because you are reimaging the Defense Center. For more information, see [Addressing Configuration Incompatibilities, page 3-7](#).

Step 2 On the Defense Center, run an events export script to create a package of intrusion and audit events; see [Exporting Events from a Version 4.10.3 Appliance, page 4-6](#).

Step 3 So they are not lost while you reimage and reconfigure the Defense Center, copy the configuration and event packages to a local computer.

Step 4 Choose one of the following options:

- If you plan to use the sensor migration script to reimage and register physical devices, continue with [Completing the Migration Using the Sensor Migration Script](#).
- If you do not plan to use the sensor migration script to reimage and register physical devices, continue with [Completing the Migration Manually, page 2-21](#).

Completing the Migration Using the Sensor Migration Script

Supported Devices: Series 2, Series 3

Supported Defense Centers: Series 2, Series 3

After exporting configurations and events from the Defense Center, you are going to reimage the Defense Center and then import your configurations. Finally, you can use the sensor migration script to reimage one or more Series 2 and Series 3 sensors, register reimaged sensors, and copy your interface configurations. If your sensors are configured to fail open, network traffic flow is not interrupted during the reimaging and configuration process.

The following sections describe the steps for completing the migration when you use the sensor migration script to reimage sensors:

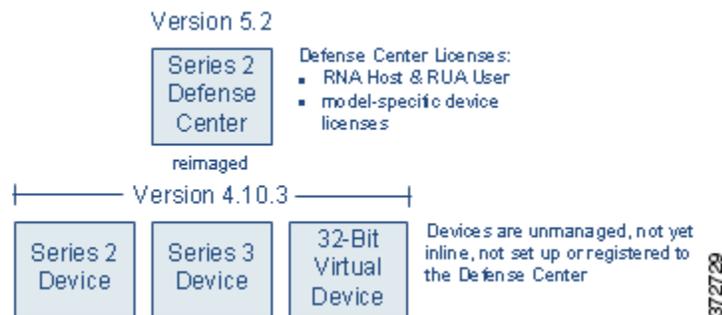
- [Reimaging the Defense Center, page 2-17.](#)
- [Importing Configurations and Events onto the Defense Center, page 2-18.](#)
- [Adding Devices to the Defense Center Using the Sensor Migration Script, page 2-19.](#)
- [Completing Device Configuration After Using the Sensor Migration Script, page 2-21.](#)

Reimaging the Defense Center

Supported Defense Centers: Series 2, Series 3

After you copy the packaged configurations and events from the Defense Center onto a local computer, you are ready to install Version 5.2 on your Defense Center. Reimaging results in the loss of almost all configuration and event data on the appliance. Although the restore utility can retain license, network, console, and Series 3 Lights-Out Management (LOM) settings, you must perform all other setup tasks after the restore process completes.

When you finish reimaging and setting up the Defense Center (including licensing), the Defense Center is ready to import configurations and events exported from Version 4.10.3.



Optionally, because you cannot reimage a virtual device (manually or by using the sensor migration script), you can also recreate the virtual sensor at this time.

To reimage your Defense Center:

Access: Admin

-
- Step 1** Using the Version 4.10.3 Defense Center's web interface (**Operations > Sensors**), remove all sensors from management.
- Step 2** Remove the virtual sensor in this scenario from the network path, and also remove any physical sensor with an inline interface that is not configured to fail open, so that traffic can continue to flow while you recreate your deployment.

Step 3 Reimage the physical Version 4.10.3 Defense Center to Version 5.2 and perform the initial setup.



Caution

Make sure you allow sufficient time for the restore process to complete. If you interrupt the process (for example, by pressing Ctrl + C or rebooting), you could cause an unrecoverable error. If you think the restore is taking too long or you experience any other issues with the process, **do not** quit, reboot, or otherwise interrupt the process. Instead, contact Support. For more information, see [CAUTION: Do Not Interrupt the Reimage Process, page 2-2](#).

For more information, see *Restoring a Sourcefire Appliance to Factory Defaults* in the [Version 5.2 Sourcefire 3D System Installation Guide](#).

Step 4 Prepare the freshly reimaged Defense Center for the import of configurations and events, as described in [Preparing for Migration, page 3-1](#).

Step 5 Optionally, create a new 64-bit virtual device using the VMware vSphere Client. Use the device's CLI to perform its initial setup.

Version 5.2 packages 64-bit virtual appliances only for the VMware ESX/ESXi hosting environment. For more information on the requirements for the hypervisor host, as well as information on creating and setting up virtual appliances, see the [Version 5.2 Sourcefire 3D System Virtual Installation Guide](#).

Step 6 Continue with [Importing Configurations and Events onto the Defense Center](#).

Importing Configurations and Events onto the Defense Center

Supported Defense Centers: Series 2, Series 3

After you reimage and set up the Defense Center, import the configurations and events you exported earlier. After you finish importing your configurations, you are ready to reimage your devices and add them to the Defense Center.



To import configurations and events onto the Defense Center:

Access: Admin

Step 1 From a local computer, copy the configuration and events export packages you exported earlier to the Version 5.2 Defense Center.

Step 2 On the Defense Center, run a script to import configurations; see [Importing Configurations onto a Version 5.2 Defense Center, page 4-7](#).

The script analyzes the configurations and, like the export script, lists those that cannot be migrated. It also gives you the opportunity to resolve any correctable issues with the imported configurations, such as detection engine-specific settings that do not migrate cleanly to Version 5.2. You also must specify some basic information for your Version 5.2 deployment, such as security zones and basic access control settings.

- Step 3** Verify the successful migration of your configurations.
For information on what to expect from migrated and new configurations, see [Understanding Migrated Configurations and Events, page 5-1](#).
- Step 4** On the Defense Center, run a script to import events; see [Importing Events onto a Version 5.2 Defense Center, page 4-20](#).
The script analyzes the event package and displays the disk space required to import the events. You can abort the import if the events require too much space, otherwise continue to import the events.
- Step 5** Continue with [Adding Devices to the Defense Center Using the Sensor Migration Script](#).
-

Adding Devices to the Defense Center Using the Sensor Migration Script

Supported Devices: Series 2, Series 3

Supported Defense Centers: Series 2, Series 3

After you import the configurations and events onto the reimaged Defense Center, you must install the sensor migration package. You are then ready to use the sensor migration script to reimage your sensors to Version 5.2. The sensor migration script copies the sensors' interface configurations, reimages the sensors, registers them to the Defense Center, and applies the interface configurations.

The script reimages and registers physical appliances, but you must recreate and register the virtual sensor in this scenario which, optionally, you could do earlier in the process (for example, while reimaging the Defense Center; see [Reimaging the Defense Center, page 2-17](#)).

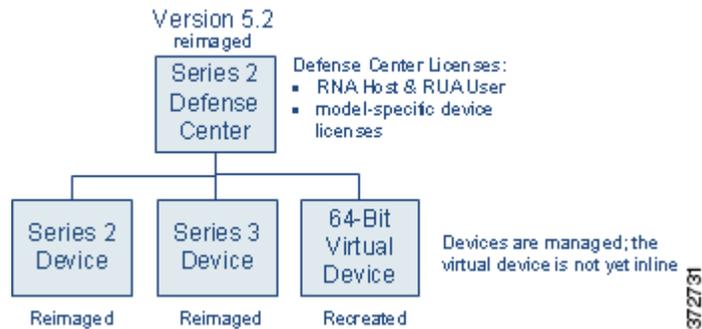
Reimaging results in the loss of almost **all** configuration and event data on the sensors. Although reimaging can retain the sensor's network, console, and Series 3 Lights-Out Management (LOM) settings, and the sensor migration script can register devices and preserve interface configurations, you must perform all other setup tasks after the restore process completes; for example, if applicable, you must reconfigure LDAP authentication.



Note

Inline interfaces **fail closed** during the reimage when you do not use the sensor migration script, or you use the script and the interfaces are not configured to fail open. In these cases, you may want to remove the sensors from your critical network path during reimage, which may require physical access to the sensors.

When you finish this phase of the migration, all sensors in your deployment are running Version 5.2 and registered. Physical devices are automatically registered and ready to establish communications. You must manually register the virtual device and, in the next phase, put it inline.



To reimage and register your sensors using the sensor migration script:

Access: Admin

- Step 1** If any Version 4.10.3 Series 2 or Series 3 inline sensor will be configured to fail closed when you reimage it, remove it from the network path so that traffic can continue to flow while you reimage it. On the Defense Center, run the sensor migration script to reimage your physical sensors; see [Reimaging and Registering Devices with the Sensor Migration Script, page 4-22](#). The script copies the Series 2 and Series 3 interface configurations, reimages the sensors, registers the reimaged sensors to the Defense Center, and applies the interface configurations.



Caution

Make sure you allow sufficient time for the restore process to complete. If you interrupt the process (for example, by pressing Ctrl + C or rebooting), you could cause an unrecoverable error. If you think the restore is taking too long or you experience any other issues with the process, **do not** quit, reboot, or otherwise interrupt the process. Instead, contact Support. For more information, see [CAUTION: Do Not Interrupt the Reimage Process, page 2-2](#).



Tip

You can specify IP addresses or host names of any physical Version 4.10.3 sensors on your network that you want to reimage and register to the Version 5.2 Defense Center, including sensors not originally registered to the Version 4.10.3 Defense Center.

- Step 2** If you did not create a new 64-bit virtual device while reimaging the Defense Center, create one now using the VMware vSphere Client. Use the device's CLI to perform its initial setup. Version 5.2 packages 64-bit virtual appliances only for the VMware ESX/ESXi hosting environment. For more information on the requirements for the hypervisor host, as well as information on creating and setting up virtual appliances, see the [Version 5.2 Sourcefire 3D System Virtual Installation Guide](#).
- Step 3** If you previously removed any inline sensors that were configured to fail closed from the network path prior to reimaging them, place the freshly set up Version 5.2 devices inline.
- Step 4** Continue with [Completing Device Configuration After Using the Sensor Migration Script](#).

Completing Device Configuration After Using the Sensor Migration Script

Supported Devices: Any

Supported Defense Centers: Series 2, Series 3

After you use the sensor migration script to reimage and register the physical sensors, and you manually recreate the virtual sensor, the final phase is to register the virtual sensor and configure all managed devices so they can begin to handle network traffic and report events to the Defense Center.

First, use the Version 5.2 Defense Center's web interface to register the virtual device, configure its interfaces, and apply the interface configurations. Then, verify the interface configurations applied by the sensor migration script. Finally, for all devices, apply the policies created and updated by the migration. For more information, see [Completing Your Version 5.2 Deployment, page 4-33](#).

Finally, place the recreated virtual device inline so it can begin handling traffic.

Completing the Migration Manually

Supported Devices: Any

Supported Defense Centers: Series 2, Series 3

Optionally, you can reimage sensors manually without using the sensor migration script. For example, you might choose to reimage manually if you have a small or low-bandwidth deployment. When you manually reimage sensors, inline sensors fail closed and physical access is often required.

The following sections describe the steps for completing the migration when you manually reimage sensors.

- [Manually Reimaging and Configuring Appliances, page 2-21](#).
- [Importing Configurations and Events onto the Defense Center, page 2-22](#).
- [Manually Adding Devices to the Defense Center, page 2-23](#).

Manually Reimaging and Configuring Appliances

Supported Devices: Any

Supported Defense Centers: Series 2, Series 3

After you copy the packaged configurations and events from the Defense Center onto a local computer, you are ready to install Version 5.2 across your deployment. You can reimage the physical appliances, but you must recreate the virtual sensor.

Reimaging results in the loss of almost **all** configuration and event data on the appliance. Although the restore utility can retain the appliance's license, network, console, and Series 3 Lights-Out Management (LOM) settings, you must perform all other setup tasks after the restore process completes.

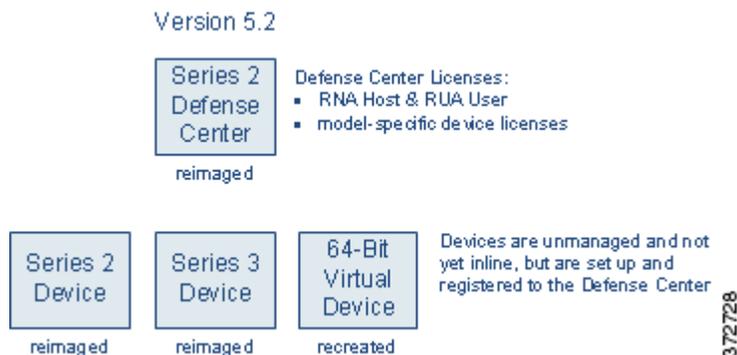


Note

Manually reimaging a sensor causes inline interfaces to fail closed until you: register the sensor to a Defense Center, and reconfigure and apply its interface configurations. You may want to disconnect inline sensors from your critical network path during the reimage. This may require physical access to the sensors.

When you do not use the sensor migration script, physical access is required to reimage Series 2 sensors, even those deployed passively; the standard Series 2 restore utility is distributed on an external USB drive. Also, when you do not use the sensor migration script, you can remotely reimage Series 3 sensors using either a remote KVM or, if enabled, LOM.

When you finish this phase of the migration, all appliances in your deployment are running Version 5.2, set up (including licensing), and ready to establish communications. The Defense Center is ready to import configurations and events exported from Version 4.10.3.



To manually reimage your deployment:

Access: Admin

-
- Step 1** Create a new 64-bit virtual device using the VMware vSphere Client. Use the device's CLI to perform its initial setup.
- Version 5.2 packages 64-bit virtual appliances only for the VMware ESX/ESXi hosting environment. For more information on the requirements for the hypervisor host, as well as information on creating and setting up virtual appliances, see the [Version 5.2 Sourcefire 3D System Virtual Installation Guide](#).
- Step 2** Using the Version 4.10.3 Defense Center's web interface (**Operations > Sensors**), remove all sensors from management.
- There is no advantage to migrating appliances one by one in this scenario.
- Step 3** Remove the sensors (including the virtual sensor) from the network path so that traffic can continue to flow while you recreate your deployment.
- Step 4** Reimage the physical Version 4.10.3 appliances to Version 5.2, and perform the initial setup.
- For more information, see the [Version 5.2 Sourcefire 3D System Installation Guide](#).
- Step 5** Prepare the freshly reimaged Defense Center for the import of configurations and events, as described in [Preparing for Migration, page 3-1](#).
- Step 6** Continue with [Importing Configurations and Events onto the Defense Center](#).
-

Importing Configurations and Events onto the Defense Center

Supported Defense Centers: Series 2, Series 3

After you reimage and set up the Defense Center, import the configurations and events you exported earlier. It is important to perform this import before you manually add devices so you can have policies and zones in place. After you finish this phase, you are ready to put devices inline and add them to the Defense Center.



To import configurations and events onto the Defense Center:

Access: Admin

-
- Step 1** From a local computer, copy the configuration and events export packages you exported earlier to the Version 5.2 Defense Center.
- Step 2** On the Defense Center, run a script to import configurations; see [Importing Configurations onto a Version 5.2 Defense Center, page 4-7](#).
- The script analyzes the configurations and, like the export script, lists those that cannot be migrated. It also gives you the opportunity to resolve any correctable issues with the imported configurations, such as detection engine-specific settings that do not migrate cleanly to Version 5.2. You also must specify some basic information for your Version 5.2 deployment, such as security zones and basic access control settings.
- Step 3** Verify the successful migration of your configurations.
- For information on what to expect from migrated and new configurations, see [Understanding Migrated Configurations and Events, page 5-1](#).
- Step 4** On the Defense Center, run a script to import events; see [Importing Events onto a Version 5.2 Defense Center, page 4-20](#).
- The script analyzes the event package and displays the disk space required to import the events. You can abort the import if the events require too much space, otherwise continue to import the events.
- Step 5** Continue with [Completing Device Configuration After Using the Sensor Migration Script](#).
-

Manually Adding Devices to the Defense Center

Supported Devices: Any

Supported Defense Centers: Series 2, Series 3

After you import configurations onto your migrated Version 5.2 Defense Center, the final step is to add and configure its managed devices so they can begin to handle network traffic and report events to the Defense Center.

First, use the Version 5.2 Defense Center's web interface to add and configure the devices, including applying licenses, adding interfaces to zones, and applying the policies created and updated by the migration. For more information, see [Completing Your Version 5.2 Deployment, page 4-33](#).

Then, place the freshly set up Version 5.2 devices (including the virtual device) inline so they can begin handling traffic.

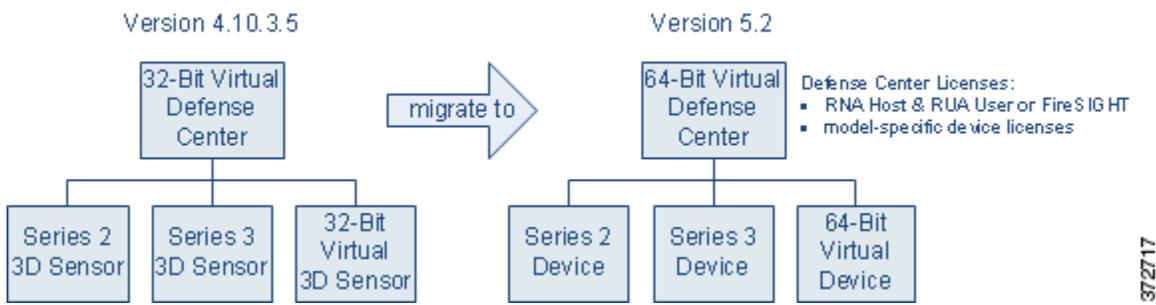
Migrating a Deployment with a Virtual Defense Center

Supported Devices: Any

Supported Defense Centers: virtual

In the scenario described in [Migrating a Simple Multi-Sensor Deployment, page 2-3](#), we replace a Version 4.10.3 Series 2 Defense Center with a Version 5.2 Series 3 Defense Center. Now, change the scenario to include a Version 4.10.3 virtual Defense Center.

The migration process is almost identical, because you must replace virtual appliances. If you want to use a virtual Defense Center to manage your Version 5.2 deployment, you must create a new 64-bit virtual Defense Center just as you must create a new virtual device.



Keep in mind that Version 5.2 packages 64-bit virtual appliances only for the VMware ESX/ESXi hosting environment. For more information on the requirements for the hypervisor host, as well as information on creating and setting up virtual appliances, see the [Version 5.2 Sourcefire 3D System Virtual Installation Guide](#).

So that this migrated deployment can behave equivalently with your Version 4.10.3 deployment, you must install the following licenses on the Version 5.2 virtual Defense Center:

- a FireSIGHT license, which replaces the RNA Host and RUA User licenses



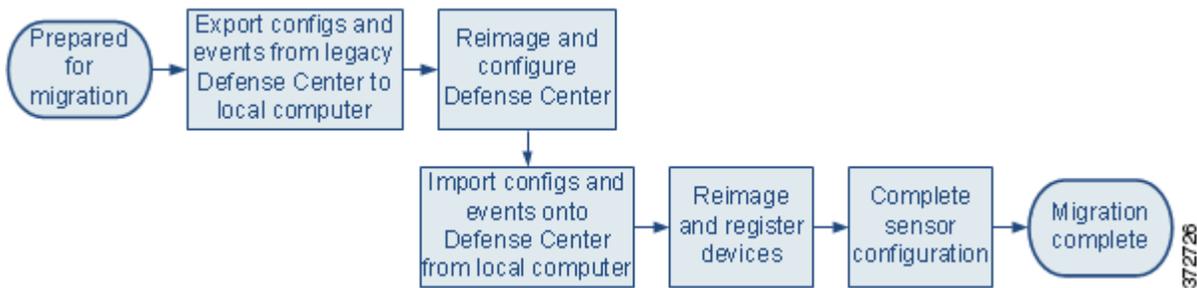
Tip

If you assign the same MAC address to the Defense Center's management interface that you used in Version 4.10.3, you can use your existing RNA Host and RUA User licenses. If you cannot use the same MAC address for the management interface (for example, the Version 4.10.3 Defense Center's MAC was dynamically assigned), you must obtain a new FireSIGHT license.

- model-specific Protection licenses for both the Series 3 and the virtual devices

You do not need a license for the Series 2 device; these devices automatically have most Protection capabilities. However, you do need a Threat & App (TA) subscription.

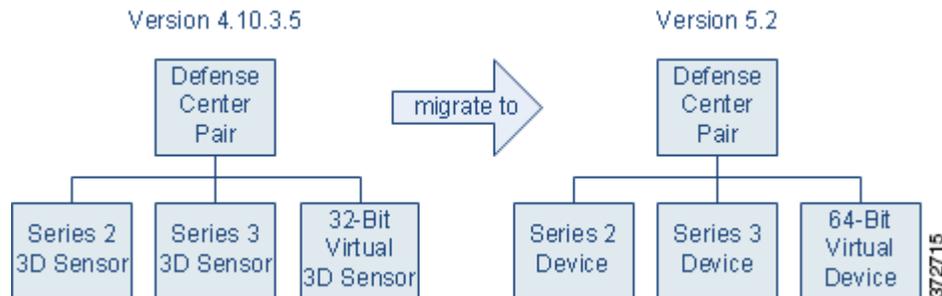
After you create and configure the replacement virtual Defense Center, you can copy configuration and event packages directly from one Defense Center to the other, then migrate the devices from the Version 4.10.3 deployment to the Version 5.2. Finally, if you want to migrate events, you can do it at the end of the process when it causes the least disruption.



Migrating High Availability Defense Center Pairs

Supported Defense Centers: DC1000, DC1500, DC3000, DC3500

Consider the simple scenario at the beginning of the chapter, [Migrating a Simple Multi-Sensor Deployment, page 2-3](#), where you migrated a simple deployment of a Defense Center managing three 3D Sensors from Version 4.10.3 to Version 5.2, while also replacing the Defense Center. Now, replace the Version 4.10.3 Defense Center with a high availability pair of Defense Centers.



How you migrate a deployment that includes a high availability pair of Defense Centers depends on whether you have a replacement Defense Center or Defense Centers. Replacing both Defense Centers in the pair is the best way to minimize downtime, and the only way to ensure that you maintain Defense Center redundancy at all times. If you do not have the resources to replace both Defense Centers, you can minimize downtime while sacrificing redundancy by using one of the pair as a temporary replacement Defense Center.



Note

Cisco **strongly** recommends that both Defense Centers in a high availability pair be the same model. Do **not** replace only one member of a pair with a different model.

Regardless of your method, keep in mind that Defense Centers in a high availability pair do not share licenses. You must obtain equivalent licenses for each member of the pair. So that this migrated high availability deployment can behave equivalently with your Version 4.10.3 deployment, you must install the following licenses on **both** Version 5.2 Defense Centers in the high availability pair:

- either a new FireSIGHT license (replacing the Defense Centers), or your RNA Host and RUA User licenses from Version 4.10.3 (using the same Defense Centers)

The RNA and RUA licenses function identically to the newer FireSIGHT license. You can obtain a FireSIGHT license for reimaged Defense Centers, but it is not required. For more information, see [Host and User Licenses, page 1-4](#).

- model-specific Protection licenses for both the Series 3 and the virtual devices

You do not need a license for the Series 2 device; these devices automatically have most Protection capabilities. However, you do need a Threat & App (TA) subscription.

For more information, see the following sections:

- [Replacing Paired Defense Centers, page 2-26](#)
- [Migrating an Existing High Availability Pair of Defense Centers, page 2-26](#)

Replacing Paired Defense Centers

Supported Defense Centers: DC1000, DC1500, DC3000, DC3500

To replace both Defense Centers, use the same basic process described in [Migrating a Simple Multi-Sensor Deployment, page 2-3](#), except instead of a single replacement Defense Center, configure a high availability pair of Version 5.2 Defense Centers.



After you prepare for the migration, create the exportable configuration package on the Version 4.10.3 primary Defense Center and copy it to the Version 5.2 primary where you can import them. The system automatically synchronizes the configurations after import. After you migrate configurations, migrate sensors, again from primary to primary.



Note

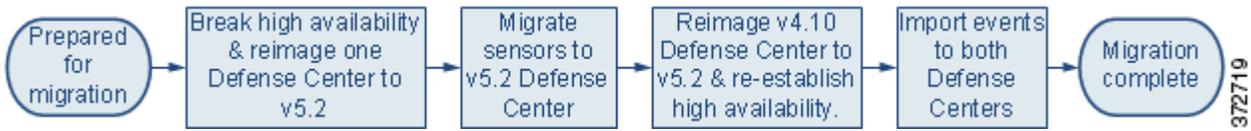
In most cases, when you reimage sensors for a high availability deployment, you can register and add the freshly configured Version 5.2 devices to only the primary Defense Center, and the system will synchronize. However, in some high availability deployments where network address translation (NAT) is used, you may need to explicitly register the device to the secondary. For more information, contact Support.

Optionally, migrate events. Unlike configurations, events are not synchronized between Defense Centers. If you want to migrate legacy events as part of your process, make sure you install the event migration scripts on both Version 5.2 Defense Centers in the replacement pair so that you can import legacy events to each one.

Migrating an Existing High Availability Pair of Defense Centers

Supported Defense Centers: DC1000, DC1500, DC3000, DC3500

If you do not have the resources to replace both Defense Centers, you can complete the migration of a high availability pair using the same basic process described in [Migrating a Simple Multi-Sensor Deployment, page 2-3](#), and using one of the pair as the replacement Defense Center, as shown in the following diagram. Note that the drawback to this scenario is that redundancy is not maintained during the process.



First, before you begin migrating configurations, disable high availability while leaving the management of the sensors active on one of the Defense Centers. Then, reimage the Defense Center that is no longer managing sensors to Version 5.2 and migrate all the sensors to that freshly reimaged Defense Center.

Reimaging results in the loss of almost all configuration and event data on the appliance. Although the restore utility can retain the appliance’s license, network, console, and Series 3 Lights-Out Management (LOM) settings, you must perform all other setup tasks after the reimage process completes.



Tip

Reimage the Defense Center that you want to act as your primary Defense Center first. If you want to continue using the same Defense Center as your primary, switch your Version 4.10.3 Defense Centers’ roles before you disable high availability. This allows the secondary Defense Center to manage the Version 4.10.3 deployment while you reimage the primary to Version 5.2.

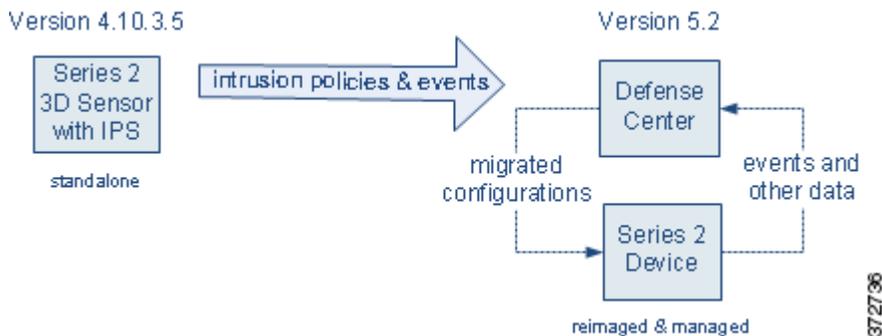
After you migrate all the sensors to the Version 5.2 Defense Center, you can reimage the remaining Version 4.10.3 Defense Center and re-establish the high availability pair using the Version 5.2 web interface. After the migrated configurations automatically synchronize, you can import legacy events onto both Defense Centers (events are not synchronized).

Migrating Standalone 3D Sensors with IPS

Supported Devices: Series 2

Standalone Series 2 3D Sensors used as an intrusion detection and prevention system (IPS) are not supported in Version 5.2. All devices must be managed by a Defense Center, and almost all configuration and analysis functions are restricted to the Defense Center. Only essential administrative and monitoring functions are available on the managed device’s web interface.

If you have a standalone Version 4.10.3 3D Sensor, you can migrate its intrusion policies and events to a Version 5.2 Defense Center. After you reimage the 3D Sensor to Version 5.2, either manually or using the sensor migration script, you can manage it with that Defense Center.



In Version 5.2, intrusion detection and prevention is integrated with access control. Instead of using the local web interface to manage a 3D Sensor with IPS and apply intrusion policies directly to detection engines, in Version 5.2 you use the Defense Center to apply access control policies to managed devices. Access control policies contain rules that determine which intrusion policy handles which traffic.

The migration process for a standalone sensor creates an access control policy on the managing Defense Center that, when applied to the migrated device, handles traffic in the same way (with a very few exceptions) as it did in Version 4.10.3.

Reimaging results in the loss of almost all configuration and event data on the sensor. The restore utility can retain the sensor's network and console settings, and the sensor migration script registers sensors and copies (but does not apply) interface configurations. However, you must perform all other setup tasks after the restore process completes.

**Note**

Inline interfaces **fail closed** during the reimage when you do not use the sensor migration script, or you use the script and the interfaces are not configured to fail open. In these cases, you may want to remove the sensors from your critical network path during reimage, which may require physical access to the sensors.

When you do not use the sensor migration script, physical access is required to reimage Series 2 sensors, even those deployed passively; the standard Series 2 restore utility is distributed on an external USB drive.

You do not need any additional licenses to manage previous standalone 3D Sensors with IPS; sensors with that capability are all Series 2, which automatically have most Protection capabilities in Version 5.2.

**Tip**

After migration, former standalone Series 2 devices can also report network discovery information to their managing Defense Center.

To migrate a standalone 3D Sensor:

Access: Admin

Step 1 Make sure you have a Version 5.2 Defense Center prepared to manage the sensor and import configurations and events.

The Defense Center can be part of your existing deployment, or can be purchased new and freshly configured. For more information, see [Preparing for Migration, page 3-1](#).

Step 2 On the sensor, run an export script to create a package of supported configurations; see [Exporting Configurations from a Version 4.10.3 Appliance, page 4-3](#).

The export script analyzes the configurations and lists those that cannot be migrated (cleanly or otherwise) to Version 5.2.

**Note**

Cisco recommends exiting the script to resolve any issues with configurations essential to your deployment. If you continue without resolving the issues, some configurations will not be migrated, though you may be able to resolve specific issues during the import process. This is especially important because you are reimaging the sensor. For more information, see [Addressing Configuration Incompatibilities, page 3-7](#).

- Step 3** On the sensor, run an export script to create a package of intrusion and audit events; see [Exporting Events from a Version 4.10.3 Appliance, page 4-6](#).
- Step 4** Copy the configuration and event packages from the Version 4.10.3 3D Sensor to the Version 5.2 Defense Center.
- Step 5** On the Defense Center, run a script to import configurations; see [Importing Configurations onto a Version 5.2 Defense Center, page 4-7](#).
- The script analyzes the configurations and, like the export script, lists those that cannot be migrated. It also gives you the opportunity to resolve any correctable issues with the imported configurations, such as detection-engine specific settings that do not migrate cleanly to Version 5.2. You also must specify some basic information for your Version 5.2 deployment, such as security zones and basic access control settings.
- Step 6** On the Defense Center, run a script to import events; see [Importing Events onto a Version 5.2 Defense Center, page 4-20](#).
- The script analyzes the package and displays the disk space required to import the events. You can abort the import if the events require too much space, otherwise continue to import the events.
- Step 7** Verify the successful migration of your configurations and events.
- For information on what to expect from migrated and new configurations, see [Understanding Migrated Configurations and Events, page 5-1](#).
- Step 8** If the Version 4.10.3 sensor is inline and is not configured to fail open, remove it from the network path so that traffic can continue to flow while you reconfigure your deployment.
- Step 9** Reimage the sensor to a Version 5.2 managed device, either manually or using the sensor migration script and, if you did not use the sensor migration script, perform the initial setup.
- For more information on manually reimaging sensors, see the [Version 5.2 Sourcefire 3D System Installation Guide](#). For more information on reimaging and registering sensors using the sensor migration script, see [Reimaging and Registering Devices with the Sensor Migration Script, page 4-22](#).
- Step 10** If you manually reimaged the device, use the Version 5.2 Defense Center's web interface to manually add the device, configure its interfaces, and apply the interface configurations.
- For more information, see [Manually Adding Version 5.2 Devices to the Defense Center, page 4-31](#).
- Step 11** For all devices, use the Version 5.2 Defense Center's web interface to apply the policies created and updated by the migration.
- For more information, see [Completing Your Version 5.2 Deployment, page 4-33](#).
- Step 12** If you removed the device from the network path before reimaging it, place it inline so it can begin handling traffic.
-



Preparing for Migration

The migration process you design for your deployment will be unique and will depend on multiple factors, including (but not limited to) the models of your appliances and your physical access to them, whether you have spare or replacement appliances to use, the number and complexity of configurations you want to migrate, whether you want to migrate events, and so on. After you read [Understanding the Migration Process, page 2-1](#) and outline how and in which order you will migrate your appliances, you can begin preparing your appliances for the migration.



Note

Cisco® Security Migration Services can help you migrate from their current security environment to a more innovative security infrastructure that provides proactive ongoing protection. Contact your Cisco representative to learn more or order Cisco Security Migration Services. See [Cisco® Security Migration Services, page 1-2](#).

Although Cisco recommends that you perform the migration in a maintenance window or at a time when the interruption will have the least impact on your deployment, the migration process can take a significant amount of time. You can minimize disruption by thoroughly preparing, but it is unlikely you will be able to avoid it completely.

For physical appliances that you reimaged to Version 5.2, you should make sure that once you start the reimage process, you have the resources and information you need to finish quickly and add the appliance to your new deployment.

If you replace a physical appliance or re-create a virtual appliance, you should **fully** set up the new appliance and **completely** prepare it to become part of your Version 5.2 deployment **before** you begin running migration scripts, changing cabling, or performing any other action that could disrupt your current deployment.



Caution

Failure to correctly prepare your appliances for migration could cause a longer than expected disruption to your deployment during the migration.

For more information on preparing appliances for migration, see:

- [Appliance, Version, and License Requirements, page 3-2](#) details the prerequisites that appliances must meet for you to perform successful migration.
- [Time and Physical Access Requirements, page 3-5](#) explains the importance of setting aside enough time for the migration and obtaining physical access to any appliances that require it for reimage, installation, or recabling.
- [Traffic Flow and Inspection During the Migration, page 3-6](#) explains how migrating your deployment can affect your organization's inspection capabilities and traffic flow.

- [Addressing Configuration Incompatibilities, page 3-7](#) explains which Version 4.10.3 configurations cannot be migrated, cleanly or otherwise, to Version 5.2, and how you can fix many of these incompatibilities before you begin the process.
- [Obtaining and Installing Migration Packages, page 3-12](#) explains how and where to obtain and install the migration scripts.

Appliance, Version, and License Requirements

Part of planning and preparing to migrate your deployment is to ensure that your current appliances and configurations are supported in Version 5.2. If they are not, your plan must account for any necessary adjustments, including hardware or virtual appliance hypervisor host replacements. For information on replacing your appliances, including an evaluation of your current and future performance needs, contact Sales.

Before you begin, you must also make sure that any existing or replacement appliances are running migration-compatible versions of the system, you have the correct licenses, and so on. Finally, you must download and install the migration scripts.

For more information on preparing your appliances for migration, see:

- [Supported Appliances, page 3-2](#)
- [Supported Source and Destination Versions for the Migration, page 3-3](#)
- [SEU and Intrusion Rule Update Requirements, page 3-3](#)
- [Version 5.2 License Requirements, page 3-4](#)
- [Disk Space Requirements, page 3-5](#)
- [Configuration and Event Backup Guidelines, page 3-5](#)

Supported Appliances

Version 5.2 is supported on all physical appliances that support Version 4.10.3. In addition, you can host 64-bit virtual appliances on VMware vSphere Hypervisor 5.0 and 5.1 as well as VMware ESX/ESXi 4.1.

The following configurations and appliances are **not** supported with Version 5.2:

- DC3000 and DC3500 appliances deployed as Master Defense Centers
- 32-bit virtual appliances on the Xen Hypervisor or RHEV hosting environments
- Crossbeam (Cisco NGIPS for Blue Coat X-Series) devices



Tip

Although Version 5.2 does not support Crossbeam (Cisco NGIPS for Blue Coat X-Series) devices, support for these devices returned with the release of Version 5.3. If your Version 4.10.3 deployment includes a Crossbeam software sensor, and you plan to upgrade to Version 5.3 or later after completing the migration, remove the sensor from the network, reimage it to Version 5.3 or later, and redeploy it in the migrated and upgraded network. For information on installing Version 5.3 or later on Cisco NGIPS for Blue Coat X-Series devices, see the *Crossbeam Installation and Configuration Guide* and the *Sourcefire 3D System Release Notes* for the version you install.

A migrated Version 5.2 deployment will function nearly equivalently to the corresponding Version 4.10.3 deployment, depending on the configurations you migrate. However, depending on the specific models of those appliances, you may not be able to take advantage of all the new features in Version 5.2 due to resource and architecture limitations.

[Supported Capabilities by Appliance Model, page 1-26](#) matches the major capabilities of the Version 5.2 system with the appliances that support those capabilities, assuming you have the correct licenses installed and applied. For information on replacing your appliances, contact Sales.

**Tip**

Although you must recreate all your virtual appliances in a 64-bit hosting environment, you can migrate legacy configurations and events to those new Version 5.2 appliances. For information on creating a new virtual appliance, including operating environment prerequisites and other details, see the [Version 5.2 Sourcefire 3D System Virtual Installation Guide](#).

Supported Source and Destination Versions for the Migration

You can use the **export scripts** to export configurations and events from any physical or virtual appliance running **Version 4.10.3.x (patch 4.10.3.5 or later)**.

You can use the **import scripts** to import configurations and events onto any physical or virtual Defense Center running **Version 5.2.0.x** of the system.

You can run the **sensor migration script** from any physical or virtual **Version 5.2.0.x** Defense Center to migrate any physical **Version 4.10.3 (or a later patch)** Series 2 or Series 3 sensor on your network to Version 5.2; this includes standalone sensors, unregistered sensors, and sensors registered to physical or virtual Defense Centers.

**Tip**

You can run the sensor migration script from a Version 5.3 Defense Center if you update the Defense Center from Version 5.2.0.x after installing the script. You cannot install the script directly on a Version 5.3 Defense Center. For example, if you want to manage Version 5.3 devices while migrating sensors, you must install the sensor migration package on your Version 5.2.0.x Defense Center before updating it to Version 5.3.

For information on updating appliances to the correct version of the system see the release notes. If you are replacing physical appliances or if your deployment includes virtual appliances (which you must re-create), see the [Version 5.2 Sourcefire 3D System Installation Guide](#) or the [Version 5.2 Sourcefire 3D System Virtual Installation Guide](#) for information on setting up new appliances.

SEU and Intrusion Rule Update Requirements

The Vulnerability and Research Team (VRT) releases Security Enhancement Updates (SEUs) to update intrusion rules and other features for Version 4.10.3. For Version 5.2, the VRT releases corresponding and comparable intrusion rule updates, also called SRUs.

The documentation accompanying each SEU identifies the corresponding rule update, and vice versa. For example, documentation for rule update 2013-08-21-001 includes the text:

Corresponding SEU number: 943

and documentation for SEU 943 includes the text:

Corresponding SRU number: 2013-08-21-001

To complete a successful migration, the SEU on the exporting Version 4.10.3 appliance **must** match the rule update on the importing Version 5.2 Defense Center. If you try to import configurations or events onto a Version 5.2 Defense Center using a package created on a Version 4.10.3 appliance running a non-matching SEU, the import fails. Note that if the documentation for your SEU or rule update does not list the corresponding partner, you **cannot** use that SEU or rule update and must import a newer one.

To ensure that the SEU and rule update match and are up-to-date, Cisco recommends that you install the latest SEU/rule update on the appliances involved in your migration, that is, on:

- **all** Version 4.10.3 standalone 3D Sensors and Defense Centers from which you plan to export configurations and events; make sure you reapply all affected intrusion policies after you update the SEU
- **all** Version 5.2 Defense Centers onto which you plan to import

For detailed instructions on importing SEUs and rule updates, see the Updating System Software chapter in the [Version 5.2 Sourcefire 3D System User Guide](#).

Version 5.2 License Requirements

Version 5.2 uses a different licensing scheme than Version 4.10.3. In Version 5.2, you use the Defense Center to control licenses for itself and the devices it manages, and most licenses from previous releases are **not** supported; see [Licensing, page 1-4](#).

At the time determined by your migration plan, add any new licenses to the appropriate Defense Centers. If you are setting up a new or reimaged physical Defense Center or a re-created virtual Defense Center, you can add licenses as part of the Version 5.2 appliance's setup process. Otherwise, you can use the Defense Center's web interface to add licenses. For more information on reimaging and setting up a new appliances, see the [Version 5.2 Sourcefire 3D System Installation Guide](#) or the [Version 5.2 Sourcefire 3D System Virtual Installation Guide](#); for information on adding licenses to the Defense Center after initial setup, see the [Version 5.2 Sourcefire 3D System User Guide](#).



Note

Your migration plan should include adding the appropriate licenses to your Version 5.2 Defense Center **before** you begin importing configurations, events, or devices. This means that **before** you begin the migration process, contact Sales for the licenses you need so that your Version 5.2 deployment can behave equivalently to your Version 4.10.3 deployment.

The following table describes which new licenses you need, if any, to migrate your deployment. Depending on your appliances, you can license additional capabilities after you complete the migration process.

Table 3-1 Licenses Required for Successful Migration

| Type | Appliance | Required Licenses in Version 5.2 |
|------------------|--|---|
| any | 3D Sensor with RNA (managed) | none |
| Series 2 | 3D Sensor with IPS, either managed or standalone | none |
| Series 3 virtual | 3D Sensor with IPS (managed) | Contact Sales for new model-specific Protection licenses to install on the managing Version 5.2 Defense Center. |

Table 3-1 Licenses Required for Successful Migration (continued)

| Type | Appliance | Required Licenses in Version 5.2 |
|----------------------|--|--|
| Series 2 Series 3 | replacement Defense Center | Contact Sales for a new FireSIGHT license. |
| Series 2 Series 3 | reimaged Defense Center | You can use legacy RNA Host and RUA User licenses instead of a FireSIGHT license. |
| virtual | replacement 64-bit Defense Center | Contact Sales for a new FireSIGHT license, unless you can assign the same MAC address to the new Defense Center's management interface that you used in Version 4.10.3. In that case, you can use your existing RNA Host and RUA User licenses. If you cannot use the same MAC address for the management interface (for example, the Version 4.10.3 Defense Center's MAC was dynamically assigned), you must obtain a new FireSIGHT license |

Disk Space Requirements

Event packages created by the migration can be large. When you run the export event script, the export fails if there is not enough space on a Version 4.10.3 appliance to create the package. Before trying again, you should free space on the appliance by deleting extraneous events, saved backup files, and so on.

Similarly, when you import events onto a Version 5.2 Defense Center, the import script warns you if you do not have enough disk space on the Defense Center to import the events in the package. Do **not** proceed if there is not enough disk space for the import; the import will fail. Before trying again, you should free space on the appliance.

Configuration and Event Backup Guidelines

Before you begin the migration process, Cisco **strongly** recommends that you back up current event and configuration data for your Version 4.10.3 deployment to an external location. Reimaging an appliance to Version 5.2 results in the loss of almost **all** configuration and event data on the appliance

When possible, use the Defense Center to back up event and configuration data for itself and the sensors it manages. For more information on the backup and restore feature, see the [Version 4.10.3 Sourcefire 3D System User Guide](#).

Time and Physical Access Requirements

Depending on the size of your deployment and the scope of your plan, the migration process can take a significant amount of time, especially if you need to reimage multiple appliances.

You can minimize disruption by thoroughly preparing, but it is unlikely you will be able to avoid it completely. Cisco **strongly** recommends you perform the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.



Caution

Failure to plan and prepare could cause a longer than expected disruption to your deployment during the migration.

Additionally, it is possible that you will need physical access to some or all of the appliances in your deployment during the migration process, depending on your appliance models, locations, and method of migration.

If you are replacing physical appliances, you must be able to install the new appliances and remove the old ones. If you are using the sensor migration script to reimage sensors, physical access is not required. If you are manually reimaging any appliances, all Series 2 appliances require physical access, as described in the following table.

Table 3-2 *Manual Reimage Requirements by Appliance Model*

| Models | Physical Access Required to Manually Reimage? |
|-------------------------------|---|
| DC1000 DC3000 | yes , to boot from and load a restore CD that contains the ISO image |
| DC500 all Series 2 devices | yes , to boot from a USB drive that contains the restore utility |
| Series 3 appliances | no ; if you have a remote KVM switch (all) or LOM (Series 3), you can remotely reimage by booting from an internal flash drive |

Additionally, reimaging an inline sensor that is not configured to fail open causes it to fail closed until you register the reimaged devices to a Defense Center and reconfigure the device's interfaces. Disconnecting inline sensors that are not configured to fail open from your critical network path during a reimage—which can take a significant amount of time—allows traffic to continue to flow, albeit uninspected.

Also, keep in mind that some migration methods require more extended physical access to your appliances than others. For example, if you have a spare device to act as a swap, you can perform a “rolling” migration that replaces each Version 4.10.3 sensor in turn. This type of rolling migration minimizes inspection downtime, because for each sensor-to-device migration you only need to interrupt traffic for the recabling. However, this scenario also requires extended physical access and moving of appliances.

By giving you an overview of the migration process for a basic scenario, then describing common variations that may apply to your deployment, [Understanding the Migration Process, page 2-1](#) can help you choose a migration method, and therefore the kind and duration of physical access you need to your appliances during the process.

Traffic Flow and Inspection During the Migration

The migration process can also affect your organization's inspection capabilities and traffic flow, especially if your plan involves reimaging your physical devices. In most cases, your available resources will dictate your course of action. You can minimize disruption by thoroughly preparing and carefully choosing a migration process, each of which has pros and cons. For more information on these and other strategies, see [Understanding the Migration Process, page 2-1](#).

Reimaging Physical Devices: More Interruption

Reimaging physical devices is cost effective, but you lose the inspection capabilities of each Series 2 and Series 3 sensor while they are being reimaged to Version 5.2.

**Note**

Inline interfaces **fail closed** during the reimage when you do not use the sensor migration script, or you use the script and the interfaces are not configured to fail open. In these cases, you may want to remove the sensors from your critical network path during reimage, which may require physical access to the sensors.

Replacing Devices: Less Interruption

Replacing physical devices minimizes inspection downtime because you can set up a parallel Version 5.2 deployment, migrate configurations, then simply switch cabling over when you are ready. However, this can be costly and requires careful planning to make sure you have the licenses, resources, and physical access to deploy multiple replacement appliances.

Because you must re-create virtual devices, traffic flow in a virtual deployment should only be interrupted while you redirect traffic to your new virtual devices.

Rolling Migration: Compromise

A “rolling” migration represents a compromise that replaces each sensor in turn. You use a replacement Defense Center to apply equivalent configurations from a Version 4.10.3 sensor to a replacement Version 5.2 device, switch cabling over from sensor to device, then reimage the now-disconnected sensor to Version 5.2 to act as the replacement device for the next Version 4.10.3 sensor.

This type of rolling migration minimizes inspection downtime, because for each sensor-to-device migration you only need to interrupt traffic for the recabling. However, this scenario also requires extended physical access and moving of appliances.

Addressing Configuration Incompatibilities

The goal of the migration is that your Version 5.2 migrated deployment behaves equivalently to your Version 4.10.3 deployment. However, there are some configurations that cannot be migrated to Version 5.2 because of deprecated functionality or functionality changes.

For your convenience, the configuration export script analyzes the exportable configurations on the appliance and lists the issues it finds. For each incompatibility, the script indicates the consequences of continuing without resolving the issue, and also lists possible solutions or workarounds. Note that you may be able to resolve some—but not all—incompatibilities when you import configurations onto the Version 5.2 Defense Center.

**Note**

If the script identifies issues, exit and resolve all critical incompatibilities before you perform a final configuration export.

Your final export from Version 4.10.3 should list only those issues that you have decided not to correct, because:

- you want to recreate specific configurations in Version 5.2,
- you do not want to migrate specific configurations, or
- you plan to resolve specific configuration conflicts when you import the package onto the Version 5.2 Defense Center (not an option for all incompatibilities)

Then, when you import a configuration package into Version 5.2, the import script again warns you of configurations in the package that cannot be migrated. If you cannot or do not want to restart the process to fix any unanticipated issues, you should have a thorough understanding of which configurations will not be migrated and why, so that you can recreate them later if necessary.

The scripts can identify, and sometimes resolve, the following migration issues:

- [Multiple Same-Type Detection Engines Using One Interface Set, page 3-8](#)
- [Intrusion Policy Proliferation Due To Custom Variables, page 3-8](#)
- [Errors Due to Unavailable Policies, page 3-9](#)
- [RNA Port Exclusion Issues, page 3-10](#)
- [Unsupported RNA and RUA Fast-Path PEP Rules, page 3-10](#)
- [Unsupported Conditions in Compliance Rules and Traffic Profiles, page 3-11](#)
- [Intrusion Rules with Ports Have No Service Metadata, page 3-11](#)

Multiple Same-Type Detection Engines Using One Interface Set

In Version 4.10.3, you could monitor one interface set with multiple IPS (or RNA or RUA) detection engines. This would allow you to, for example, analyze the same traffic with multiple intrusion policies.

Version 5.2 does not support this capability. Now, you apply one access control policy to a device. In that access control policy, if traffic matches an access control rule you can analyze it with one intrusion policy; if it matches no rules, you can analyze it with a different intrusion policy (the default action policy).

To resolve this issue before you export Version 4.10.3 configurations, modify your deployment so that only one of each type of detection engine uses each interface set. For instructions, see the [Using Detection Engines and Interface Sets](#) chapter in the *Version 4.10.3 Sourcefire 3D System User Guide*.

If you export Version 4.10.3 configurations where more than one IPS or RNA detection engine monitored the same interface, the configuration import script prompts you to choose one; for more information, see [Assigning One Detection Engine of Each Type to Interface Sets, page 4-10](#).

Choosing an RNA or IPS detection engine uses the policy that was applied to that detection engine as a basis for your Version 5.2 configurations. Although it is unlikely that you were using more than one RUA detection engine to monitor the same traffic (because there was no advantage to doing so), the script automatically chooses just one of them to use for Version 5.2.

Intrusion Policy Proliferation Due To Custom Variables

In the Sourcefire 3D System a variable is a representation of a port or network value that is commonly used in intrusion rules. Rather than hard-coding these values in multiple rules, to tailor a rule to accurately reflect your network environment, you can change the variable value.

In Version 4.10.3 you could configure custom variables for IPS detection engines, which had priority over intrusion policy-specific variables which, in turn, had priority over system variables. With Version 5.2, you no longer explicitly configure detection engines or detection engine variables; however, you still can configure policy-specific variables, which still have priority over system variables. However, this means that you cannot cleanly migrate a Version 4.10.3 intrusion policy applied to IPS detection engines that use custom variables.

To replicate Version 4.10.3 functionality and migrate custom detection engine variables, the import script can create a copy of the intrusion policy for each detection engine that uses custom variables. These copies use the original intrusion policy as the base policy; each one has different policy-specific variables that correspond to one of the Version 4.10.3 custom variable sets.

Because this can result in a proliferation of intrusion policies, the import script prompts you whether to create the copies; see [Creating Intrusion Policies For Custom Detection Engine Variables, page 4-11](#). For details on how custom detection engine variables appear after they are migrated, see [Migrating Detection Engine Variables Into Policy Variables, page 5-7](#).

To resolve this issue before you export Version 4.10.3 configurations, make sure you do not use IPS detection-engine variables. Your solution may be to create a copy of the intrusion policy for each detection engine that uses custom variables, just as the import script would. Or, you can delete detection engine variables if you do not plan to need them in your Version 5.2 deployment. For instructions, see the Using Detection Engines and Interface Sets chapter in the [Version 4.10.3 Sourcefire 3D System User Guide](#).

Errors Due to Unavailable Policies

You can only migrate intrusion policies that were created on (or imported onto) a Version 4.10.3 appliance, that currently exist on the appliance, and that are currently applied to IPS detection engines. Similarly, you can only migrate settings from RNA detection policies, RNA-related settings in system policies, and PEP policies if they exist (and if necessary, are applied) on an exporting Version 4.10.3 Defense Center.

You **cannot** migrate the following:

- a remotely-authored intrusion policy, that is, an intrusion policy that is applied to an IPS detection engine from an appliance other than the one from which you are exporting configurations
- applied-then-deleted intrusion policies
- settings from applied-then-deleted policies: PEP, system, and RNA detection policies
- occasionally, settings from applied-then-modified system policies

Both the configuration export and import scripts warn you that these policies and settings will not be migrated, and give you a chance to exit the script. Not importing these configurations can cause the omission of rules and other important settings from the new access control policy and the network discovery policy on the Version 5.2 Defense Center.

Note, however, that the migration attempts to resolve unavailable and conflicting system policy settings in the following ways:

- If another version of the currently applied system policy exists on the Version 4.10.3 Defense Center (for example, you modified the policy since you last applied it and a saved revision exists), the migration uses the settings in the saved revision.
- If you deleted the currently applied system policy, the migration uses the existing settings on the Version 5.2 Defense Center that the configuration import script would otherwise overwrite; see [Understanding How RNA and RUA Settings Are Migrated, page 5-13](#).

To resolve this issue before you export Version 4.10.3 configurations, apply the policies that you want to migrate to the appropriate sensors, detection engines, or interface sets. Note that you do not have to apply compliance policies. For instructions, see the [Version 4.10.3 Sourcefire 3D System User Guide](#).

RNA Port Exclusion Issues

In Version 4.10.3, you configured host discovery and flow data logging in RNA detection policies, and could easily exclude a port associated with a specific IP address from having its sessions logged.

In Version 5.2, logging and monitoring functionality is split: the access control policy governs which connections (flows) are logged on a per-access-control-rule basis, but the network discovery policy governs host discovery. Access control rules also define the traffic that you allow, and only traffic that you allow (as opposed to outright block or trust) can be monitored with discovery or subject to an intrusion policy.

To exclude traffic to and from a specific host from connection logging while preserving logging and inspection for other hosts, the script must create multiple access control rules for combinations of intrusion inspection and port exclusion preferences; see [Migrating RNA Settings into Rules and Logging Preferences](#), page 5-7.

If your Version 4.10.3 RNA detection policies specified **Source/Destination** ports to exclude, the import scripts prompts you to choose whether to create these extra rules in the new access control policy, for example. To avoid a confusing proliferation of rules, the default option is to create the access control policy without them.

However, you cannot migrate source-only or destination port exclusions. If your Version 4.10.3 RNA detection policies specifies either **Source** or **Destination** ports to exclude, the script warns you that these configurations will not be migrated.

To resolve these issues before you export Version 4.10.3 configurations, modify the port exclusions in your RNA detection policies, then reapply the policies. For instructions, see the Introduction to Sourcefire RNA chapter in the [Version 4.10.3 Sourcefire 3D System User Guide](#).



Tip

For information on configuring port exclusions in Version 5.2 using discovery rules, see the Introduction to Network Discovery chapter in the [Version 5.2 Sourcefire 3D System User Guide](#).

Unsupported RNA and RUA Fast-Path PEP Rules

Version 4.10.3 PEP rules with an action of **Fast Path** are migrated to Version 5.2 as access control rules that trust the specified traffic. For information on how other types of PEP rule are migrated, see [Migrating PEP Rules into Access Control Rules](#), page 5-3.

Because of the way Version 5.2 access control rules handle traffic, you cannot configure traffic to bypass discovery (RNA or RUA) but still be analyzed by an intrusion policy (IPS). Therefore, Version 4.10.3 RNA and RUA fast-path PEP rules **cannot** be migrated unless you also fast-path IPS.

To resolve this issue before you export Version 4.10.3 configurations, delete or modify unsupported PEP rules. For instructions, see the *Using PEP to Manage Traffic* chapter in the [Version 4.10.3 Sourcefire 3D System User Guide](#).

If you export these Version 4.10.3 PEP rules, the configuration import script prompts you to resolve the issue by either deleting the configuration, bypassing intrusion inspection only, or bypassing all inspection. You **cannot** migrate the PEP rule as-is. For more information, see [Resolving Unsupported RNA and RUA Fast-Path PEP Rules](#), page 4-12.

Unsupported Conditions in Compliance Rules and Traffic Profiles

In Version 5.2, the Policy & Response and compliance features are known as *correlation features*. You can successfully migrate most compliance policies and rules to Version 5.2 correlation policies and rules; see [Understanding Migrated Compliance Policies and Rules, page 5-18](#). Most traffic profiles also migrate successfully.

The Policy & Responses configurations that you **cannot** migrate are detailed in the following table. Both the configuration export and import scripts warn you that these configurations will not be migrated, and give you a chance to exit the script.

Table 3-3 *Unsupported Conditions in Compliance Rules and Traffic Profiles*

| You cannot migrate a... | Where... | Because... |
|-------------------------|--|---|
| compliance rule | an RNA event occurs using a Detection Engine constraint | the migration script cannot create a Version 5.2 discovery-based correlation rule using a Device constraint until you add devices to the Defense Center, which you do after you run the import script. |
| compliance rule | an RNA event occurs or a flow event occurs using an Application Type or Payload Type constraint | in Version 5.2, you cannot trigger correlation rules based on application categories and tags, which are the Version 5.2 analogs for application and payload types. |
| traffic profile | a host profile qualification using a Client Application constraint where you specify one or more Application Type (other than any) | in Version 5.2, you cannot track connections based on application categories and tags, which are the Version 5.2 analogs for application and payload types. |
| traffic profile | a host profile qualification using a Client Application constraint where you specify an Application of any | in Version 5.2, you cannot track connections based on a Client of any ; you must explicitly choose one or more client applications. |

To resolve these issues before you export Version 4.10.3 configurations, you must modify your compliance rules and traffic profiles so that they no longer use the unsupported conditions. For instructions, see the Configuring Compliance Policies and Rules and Working With Flow Data and Traffic Profiles chapters in the [Version 4.10.3 Sourcefire 3D System User Guide](#).



Tip

You can re-create discovery-based device-specific correlation rules on your Version 5.2 Defense Center after you complete the migration process.

Intrusion Rules with Ports Have No Service Metadata

In Version 4.10.3, local intrusion rules that inspect traffic only on specified ports do so regardless of the application detected in the traffic. In Version 5.2, for an intrusion rule to inspect application traffic, that rule **must** include a service metadata option for the identified application.

The configuration import script identifies local intrusion rules that have port constraints but no corresponding service metadata, and generates one or more service metadata recommendations based on the rule content. Then, the script prompts you to accept, review, or reject the recommendations; see [Adding Service Metadata to Intrusion Rules, page 4-11](#). Note that you **cannot** use the script to add more than eight metadata entries; the script presents the first eight, alphabetically. You can add additional metadata before or after the migration.

**Note**

Skipping (rejecting) the addition of service metadata will stop the affected intrusion rules from firing until you add service metadata after the migration. For more information, see the Understanding and Writing Intrusion Rules chapter in the [Version 5.2 Sourcefire 3D System User Guide](#).

Note that the script does not allow you to review or automatically add service metadata to local intrusion rules that inspect traffic based on port negations; this would be too complex. For these rules to fire, you **must** manually add service metadata after the migration. The script warns you which rules need this manual update.

To resolve these issues before you export Version 4.10.3 configurations, add service metadata to all local intrusion rules that have port constraints, including port negations. For instructions, see the Understanding and Writing Intrusion Rules chapter of your [Version 4.10.3 Sourcefire 3D System User Guide](#).

Obtaining and Installing Migration Packages

Cisco delivers migration scripts in appliance-specific packages. To install the scripts, you must install the correct package for your appliance type. The packages include the following scripts:

- An appliance-specific **export package** contains the configuration export script and the event export script.

You must download and install the export package on every **Version 4.10.3.x (patch 4.10.3.5 or later)** Defense Center or standalone sensor where you want to run the configuration and event export scripts.

- An appliance-specific **import package** contains the configuration import script and the event import script.

You must download and install the import package on every **Version 5.2.0.x** Defense Center where you want to run the configuration and event import scripts.

- A Defense Center series-specific **sensor migration package** contains the sensor migration script.

You must download and install the sensor migration package on every **Version 5.2.0.x** Defense Center where you want to run the sensor migration script.

**Tip**

In a high availability deployment, you only need to install the import package on the primary Defense Center, unless you want to import events onto both Defense Centers in the pair.

The following table lists the packages you must install to use the migration scripts on each appliance:

Table 3-4 Migration Script Packages by Appliance

| Package Type | Appliance | Package |
|--------------|--|--|
| export | Series 2 Defense Center 32-bit virtual Defense Center | Sourcefire_3D_DC_Migration_Export_Package-4.10.3.999-build.sh |
| export | Series 3 Defense Center | Sourcefire_3D_Defense_Center_S3_Migration_Export_Package-4.10.3.999-build.sh |
| export | standalone Series 2 3D Sensors | Sourcefire_3D_Sensor_Migration_Export_Package-4.10.3.999-build.sh |

Table 3-4 Migration Script Packages by Appliance (continued)

| Package Type | Appliance | Package |
|--------------|--|---|
| export | standalone 3D9900 3D Sensors Note that the 3D9900 is no longer supported; however, you can use this script to export configurations and events from a Version 4.10.3 standalone 3D9900. | Sourcefire_3D_Sensor_9900_Migration_Export_Package-4.10.3.999-build.sh |
| import | Series 2 Defense Center | Sourcefire_3D_DC_Migration_Import_Package-5.2.0.999-build.sh |
| import | Series 3 Defense Center 64-bit virtual Defense Center | Sourcefire_3D_Defense_Center_S3_Migration_Import_Package-5.2.0.999-build.sh |
| sensor | physical Series 2 Defense Center | Sourcefire_3D_DC_Sensor-Migration-Hotfix-5.2.0.999-build.sh |
| sensor | physical Series 3 Defense Center 64-bit virtual Defense Center | Sourcefire_3D_Defense_Center_S3_Sensor-Migration-Hotfix-5.2.0.999-build.sh |

To install migration packages:**Access:** Admin**Step 1** Using the user name and password for your support account, log into the Support Site.**Step 2** Download the appropriate script package from the Support Site.For information on which package to download, see [Table 3-4 on page 3-12](#).**Caution**

Download each script package directly from the Support Site. If you transfer a script package by email, it may become corrupted.

Step 3 On each appliance where you need to run a migration script, upload the appropriate script package:

- to upload the export package to a Version 4.10.3 (patch 4.10.3.5 or later) Defense Center or standalone sensor, select **Operations > Update**, then click **Upload Update**. Browse to the package and click **Upload**.
- to upload the import or sensor migration package to a Version 5.2 Defense Center, select **System > Updates**, then click **Upload Update** on the Product Updates tab. Browse to the package and click **Upload**.

Step 4 Click **Install** next to the package you are installing.The package is installed and the script or scripts are ready to be run. For information on running each script, see [Performing the Migration, page 4-1](#).



Performing the Migration

Obtaining and installing migration packages is the last step in preparing for your deployment's migration, as described in [Obtaining and Installing Migration Packages, page 3-12](#). After you install these packages, you can run each script included in the packages at the appropriate time.



Note

The order in which and appliances where you run migration scripts depends on your migration plan, which is unique to your deployment. Make sure you adhere to your plan by running the migration scripts and performing related tasks in the correct order. In particular: migrating events before you migrate configurations can result in unpredictable event display and behavior; also, the order in which you reimage and register devices depends on whether you reimage using the sensor migration script. For more information on the order in which you should migrate configurations and events in your situation, see [Understanding the Migration Process, page 2-1](#).

The following table lists each script and its function.

Table 4-1 Migration Scripts

| Use this script... | To... |
|---|---|
| configuration export: <code>config_export.pl</code> | create an exportable package of configurations on a Version 4.10.3 Defense Center or standalone 3D Sensor |
| event export: <code>event_export.pl</code> | create an exportable package of intrusion and audit events on a Version 4.10.3 Defense Center or standalone 3D Sensor |
| configuration import: <code>config_import.pl</code> | import configurations onto a Version 5.2 Defense Center |
| event import: <code>event_import.pl</code> | import events onto a Version 5.2 Defense Center |
| display interfaces: <code>display_interfaces.pl</code> | display interface configurations after running the configuration import script; this script is not necessary when you use the sensor migration script, but is useful when you must manually configure interfaces on physical devices that you manually reimaged or virtual devices that you created |
| migrate sensors: <code>migration_script.pm</code> | copy Version 4.10.3 (or a later patch) Series 2 and Series 3 physical sensor interface configurations, reimage the sensors to Version 5.2, register them to the Version 5.2 Defense Center where you run the script, and apply the interface configurations |

To run any migration script, you must be logged into the appliance's shell. You must have Administrator access to the appliance and run the script as the root user. For most appliances, you can use SSH to connect to the appliance; for virtual appliances you can also use the virtual console. You can also connect to the Series 3 appliance shell via Lights-Out Management (LOM).

Depending on the script and the options you use to invoke it, you may need to provide input as the script runs. When prompted, either type the requested information or the number corresponding to your choice and press Enter to continue. You can also just press Enter to accept the default, which is displayed in brackets.

For example, the configuration import script asks you to provide a name for the new access control policy created by the import:

```
Enter the new Access Control policy name [Migrated policy]:
```

In this case, you can either type a name for the new policy, or press Enter to accept the default name of `Migrated policy`. Invalid input causes the scripts to re-prompt you for valid input.



Tip

This chapter explains in detail how to run each of the migration scripts, but you can get basic instructions and syntax by running any of the scripts with the `--help` option; for example: `config_export.pl --help`.

This chapter also provides details on reimaging appliances as part of the migration, and performing the initial setup on those and any replacement appliances you are using in your new Version 5.2 deployment.

For more information, see:

- [Logging Into an Appliance to Run Migration Scripts, page 4-2](#)
- [Exporting Configurations from a Version 4.10.3 Appliance, page 4-3](#)
- [Exporting Events from a Version 4.10.3 Appliance, page 4-6](#)
- [Importing Configurations onto a Version 5.2 Defense Center, page 4-7](#)
- [Importing Events onto a Version 5.2 Defense Center, page 4-20](#)
- [Rebuilding Version 4.10.3 Appliances, page 4-21](#)
- [Completing Your Version 5.2 Deployment, page 4-33](#)
- [Next Steps, page 4-39](#)

Logging Into an Appliance to Run Migration Scripts

To run any migration script, you must be logged into the appliance's shell. You must have Administrator access to the appliance and run the script as the root user. For most appliances, you can use SSH to connect to the appliance; for virtual appliances you can also use the virtual console. You can also connect to the Series 3 appliance shell via Lights-Out Management (LOM).



Note

Before you can run migration scripts using LOM, you must enable the feature on the appliance and install an IPMI utility on your computer. Keep in mind that the syntax of LOM commands depends on the utility you are using. For more information on LOM, including a full list of available commands,

To log into a Series 3 appliance using Lights-Out Management:

Access: Admin

Step 1 At your computer's command prompt, enter the IPMI command to start a Serial over LAN (SOL) session and display the prompt for the appliance:

- For IPMITool, type: `ipmitool -I lanplus -H IP_address -U username sol activate`
- For ipmiutil, type: `ipmiutil sol -a -V4 -J3 -N IP_address -U username -P password`

Where *IP_address* is the IP address of the management interface on the appliance, *username* is the user name of an authorized LOM account, and *password* is the password for that account.

Note that IPMITool prompts you for the password after you issue the `sol activate` command.

Exporting Configurations from a Version 4.10.3 Appliance

Supported Devices: Series 2

Supported Defense Centers: Any

After you prepare for migration, the next step is to export vital configurations from your Version 4.10.3 Defense Centers and standalone 3D Sensors. To export configurations from an appliance, log into its shell and run a script that creates an export package:

- On a standalone 3D Sensor, the package contains information on applied intrusion policies and their associated variables.
- On a Defense Center, the package contains information on applied intrusion policies and their associated variables for all managed sensors, RNA and RUA settings and policies, PEP rules, as well as compliance policies, rules, and traffic profiles.

For more information on exactly what is migrated, see [Understanding Migrated Configurations and Events, page 5-1](#).

When you start the configuration export script, it analyzes the exportable configurations on the appliance and lists any configurations that cannot be migrated, cleanly or otherwise, to Version 5.2. For each incompatibility, the script indicates the consequences of continuing without resolving the issue, and also lists possible solutions or workarounds.

The following table displays the issues the script can detect, and directs you to documentation where you can learn about why the problem exists and what you can do to correct it.

Table 4-2 Migration Issues Identified by the Configuration Export Script

| Issue | For more information, see... |
|--|--|
| Multiple <i>DE_type</i> detection engines are using interface set ' <i>set_name</i> ' from sensor <i>sensor_name</i> . | Multiple Same-Type Detection Engines Using One Interface Set, page 3-8 |
| Intrusion Policies with customized variable definitions must be created in order to accurately migrate Detection Engine variables. | Intrusion Policy Proliferation Due To Custom Variables, page 3-8 |

Table 4-2 Migration Issues Identified by the Configuration Export Script (continued)

| Issue | For more information, see... |
|---|---|
| <p>The following remotely authored intrusion policies are applied to IPS detection engines:</p> <p>These intrusion policies have been deleted but are applied to IPS detection engines:</p> <p>The RNA policy applied to '<i>detection_engine</i>' on sensor <i>sensor_name</i> was deleted and cannot be migrated.</p> <p>The PEP policy applied to '<i>interface_set</i>' on sensor <i>sensor_name</i> was deleted and cannot be migrated.</p> <p>The applied System Policy revision cannot be found. The latest revision will be used.</p> <p>The applied System Policy cannot be found. Network Discovery settings will use the installed defaults.</p> | <p>Errors Due to Unavailable Policies, page 3-9</p> |
| <p>These RNA port exclusions are not compatible with network discovery in 5.2.0 because they target either a source network or a destination network (not both source and destination):</p> | <p>RNA Port Exclusion Issues, page 3-10</p> |
| <p>PEP rules have been found that have an action of 'DE-specific' and are configured to fast path RNA or RUA:</p> | <p>Unsupported RNA and RUA Fast-Path PEP Rules, page 3-10</p> |
| <p>These compliance rules are not compatible with 5.2.0 because they contain a '<i>condition_type</i>' condition.</p> <p>These traffic profiles are not compatible with 5.2.0 because they contain a '<i>condition_type</i>' condition.</p> | <p>Unsupported Conditions in Compliance Rules and Traffic Profiles, page 3-11</p> |

If the script identifies issues, Cisco recommends that you exit and resolve all critical incompatibilities before you perform a final export. Your final export should list only those issues that you have decided not to correct, because either you want to recreate the configurations in Version 5.2, or you do not want to migrate those configurations. Note that in some cases, you may be able to resolve some issues during the import process.

Every time you run the script without exiting, it creates a new export package— unless you specify otherwise, a timestamped compressed archive (.tgz) file in the migration directory on the appliance. For example, a file created at 1:14:15 PM on January 1, 2014 would be located at:

```
/var/sf/migration/migration_config_20140101_131415.tgz
```

**Note**

Before you run the configuration export script on a Version 4.10.3 Defense Center, make sure that the appliances in your deployment are communicating successfully. If the Defense Center cannot contact one of its managed sensors, it cannot include its interface information in the package.

The following table describes the options you can use with the configuration export script.

Table 4-3 Configuration Export Script Options

| Option | Description |
|--------|--|
| --file | Create a new export package with a specified file name and location, instead of the default. You can use an absolute or relative path, for example: <pre>--file ./export_1/my_export.tgz --file /var/sf/migration/export_1/my_export.tgz</pre> If the directory you specify does not exist, the script automatically creates it. Note that if you specify the same name and location as an existing export package, the older package is overwritten. |
| --help | Display basic instructions and syntax for running the script. |

To create an export package of configurations:**Access:** Admin

-
- Step 1** Log into the appliance's shell using an account with Administrator privileges.
For more information, see [Logging Into an Appliance to Run Migration Scripts](#), page 4-2.
- Step 2** Navigate to the migration folder:
- ```
cd /var/sf/migration
```
- Step 3** Run the export script as the root user, providing your password when prompted:
- ```
sudo ./config_export.pl
```
- Use the `--file` option to specify an alternate location or file name for the export package. For more information on the other options you can use, see [Configuration Import Script Syntax and Options](#), page 4-17.
- After you provide your password, the script starts and lists any configuration incompatibilities with the migration:
- ```
Migration Export Assistant v1.0
SOURCEfire, inc.
=====
Analyzing configuration.....
The following issues were detected:
```
- Step 4** Read and understand the list of issues, if any.  
To cross reference an issue displayed with information on how to correct it, see [Table 4-2 on page 4-3](#).
- Step 5** When prompted, type `y` to continue or `n` to exit the export process, then press Enter.  
Cisco recommends exiting the script to resolve any issues with configurations essential to your deployment. If you continue, the script gathers data from the appliance (and, for a Defense Center, its managed sensors), creates the export package, and exits, for example:
- ```
Do you want to continue the export process? (y/n) [n]: y
Collecting data from sensors...
Gathering data for My_4.10.3_Defense_Center...
Creating migration backup...
Migration export complete!
migration_config_20140101_131415.tgz created.
```
- Step 6** Continue with the next step in your migration plan.
For more information on planning your migration, see [Understanding the Migration Process](#), page 2-1.
-

Exporting Events from a Version 4.10.3 Appliance

Supported Devices: Series 2

Supported Defense Centers: Any

If you are interested in intrusion and audit events generated in your Version 4.10.3 deployment before the migration, you can migrate these legacy events from Version 4.10.3 Defense Centers and standalone 3D Sensors.

To export events from an appliance, log into its shell and run a script that creates an export package, which contains all intrusion events and audit events on the appliance at the time. You can then copy and import the event package onto a Version 5.2 Defense Center.

When you start the script on a Defense Center, it first determines whether you are still managing any sensors and, if so, allows you to exit. Depending on your migration plan, you may actually want to export events and then remove sensors from management (for example, if you are reimaging an existing Defense Center that is managing sensors that you plan to remove from the network path because they would fail closed). However, keep in mind that events reported to the Defense Center after you start the export process are not included in the package. For more information on planning your migration, see [Understanding the Migration Process, page 2-1](#).

Every time you run the script without exiting, it creates a new export package— unless you specify otherwise, a timestamped compressed archive (.tgz) file in the migration directory on the appliance. For example, a file created at 1:14:15 PM on January 1, 2014 would be located at:

```
/var/sf/migration/migration_event_20140101_131415.tgz
```

The following table explains the options you can use with the event export script.

Table 4-4 *Event Export Script Options*

| Option | Description |
|--------|---|
| --file | Create a new export package with a specified file name and location. You can use an absolute or relative path, for example: <pre>--file ./export_1/my_export.tgz</pre> <pre>--file /var/sf/migration/export_1/my_export.tgz</pre> If the directory you specify does not exist, the script automatically creates it. Note that if you specify the same name and location as an existing export package, the older package is overwritten. |
| --test | Runs the script but does not create the event package. This allows you to preview what will happen when you run the final export. |
| --help | Display basic instructions and syntax for running the script. |

Note that if there is not enough space on the appliance to create the export package, the export fails. Before you try again, free space on the appliance by deleting extraneous events, saved backup files, and so on.

Also, keep in mind that some fields in intrusion events generated by Version 4.10.3 are different from the fields in Version 5.2 intrusion events, and that the timestamps on migrated events will be “behind” newly generated events. For information on how legacy events appear in the Version 5.2 web interface, see [Understanding Migrated Intrusion and Audit Events, page 5-18](#).

To create an export package of intrusion and audit events:

Access: Admin

-
- Step 1** Log into the appliance's shell using an account with Administrator privileges.
For more information, see [Logging Into an Appliance to Run Migration Scripts, page 4-2](#).
- Step 2** Navigate to the migration folder:
- ```
cd /var/sf/migration
```
- Step 3** Run the export script as the root user, providing your password when prompted:
- ```
sudo ./event_export.pl
```
- Use the `--file` option to specify an alternate location or file name for the export package. For more information on the other options you can use, see [Table 4-4Event Export Script Options, page 4-6](#).
After you provide your password, the script starts:
- ```
Migration Event Export Assistant v1.0
SOURCEfire, inc.
=====
```
- Step 4** On a Defense Center that is still managing 3D Sensors, if prompted whether you want to continue the export process, enter `y` to continue or `n` to exit.
- ```
This DC has at least one sensor attached.
Are you sure you want to export events now? (y/n) [y]:
```
- Step 5** Wait until the export script completes and creates the export package, for example:
- ```
Dumping mysql tables...
Archiving audit events...
Archiving IS events...
Creating event migration backup...
migration_event_20140101_131415.tgz created.
```
- Step 6** Continue with the next step in your migration plan.  
For more information on planning your migration, see [Understanding the Migration Process, page 2-1](#).
- 

## Importing Configurations onto a Version 5.2 Defense Center

**Supported Devices:** None

**Supported Defense Centers:** Any

After you export configurations from your Version 4.10.3 deployment and ready your Version 5.2 Defense Center, your next step is to import the configurations. First, copy a Version 4.10.3 configuration package (see [Exporting Configurations from a Version 4.10.3 Appliance, page 4-3](#)) to the new Defense Center. Then, run an interactive script that steps you through the import of the configurations in the package, using a series of checks and requests for input.

You should run the import script once for each configuration package you need to import:

- If you are migrating from a single Version 4.10.3 Defense Center to a single Version 5.2 Defense Center, you should only have one configuration package to import.
- If you are replacing two or more Version 4.10.3 Defense Centers with one Version 5.2 Defense Center, or are adding several former standalone 3D Sensors to a new Defense Center, you must import each configuration package individually.

Before you commit to importing configurations from a specific exported package, you can run the import script using the `--manifest` option to display a detailed list of the Version 4.10.3 configurations in that package. If a review of the manifest reveals anything unexpected, Cisco recommends that you fix critical issues and export a new package from the Version 4.10.3 appliance, if possible. For more information on reviewing the manifest, see [Reviewing the Manifest of Exported Configurations, page 4-9](#).

Also note that when you run the import script, it cleans up information from any previous invocations. If you import multiple configuration packages, each import deletes useful information on how to configure migrated devices associated with previously imported packages. For more information, see [Importing Multiple Unique Configuration Packages, page 4-18](#).

The following sections explain how to run and follow the prompts in the configuration import script:

- [Starting the Configuration Import Script, page 4-8](#)
- [Reviewing the Manifest of Exported Configurations, page 4-9](#)
- [Verifying Configuration Incompatibilities, page 4-9](#)
- [Resolving Configuration Conflicts, page 4-10](#)
- [Creating Security Zones Based on Interface Sets, page 4-13](#)
- [Providing Basic Access Control Settings, page 4-15](#)
- [Verifying the Migrated Configuration, page 4-16](#)
- [Confirming the Import and Resolving Configuration Collisions, page 4-16](#)

The following sections provide additional information about the import script:

- [Configuration Import Script Syntax and Options, page 4-17](#)
- [Importing Configurations Multiple Times, page 4-18](#)

## Starting the Configuration Import Script

When you start the configuration import script on a Version 5.2 Defense Center, it first compares the intrusion rule update on the Defense Center to the SEU on the Version 4.10.3 appliance where you exported the package. If the rule update and SEU do not match, the script exits without importing any configurations. Cisco **strongly** recommends that you update the SEUs and rule updates in your deployment and restart the migration process. For more information, see [SEU and Intrusion Rule Update Requirements, page 3-3](#).

If you cannot restart the migration process because you have already reimaged the appliance where you exported the package, you can force the script to skip the equivalence check by invoking the script with the `--force` option. In most cases, the resulting imported intrusion configurations will work as expected. If you cannot edit or apply policies after forcing a configuration import, contact Support.



### Note

If this is the second time you plan to run the import script on this Defense Center, **regardless** of whether you are re-importing configurations from the same package or you are importing new configurations from a different package, read the warnings in [Importing Configurations Multiple Times, page 4-18](#).

### To begin importing migrated configurations onto a Version 5.2 Defense Center:

**Access:** Admin

- 
- Step 1** Copy the package you plan to import to the Version 5.2 Defense Center. Cisco recommends that you copy all packages to the `/var/sf/migration` directory.
- Step 2** Log into the Defense Center's shell using an account with Administrator privileges. For more information, see [Logging Into an Appliance to Run Migration Scripts, page 4-2](#).
- Step 3** Navigate to the migration directory:

**Step 4** Run the import script as the root user, providing your password when prompted:

```
cd /var/sf/migration
```

```
sudo ./config_import.pl exported_config_package.tgz
```

where `exported_config_package.tgz` is the package you copied to the Defense Center. If you did not copy the package to the migration directory, make sure you provide a relative or absolute path to the package.

After you provide your password, the script starts. If the Defense Center passes the rule update equivalence check, the script collects data from the package and performs any necessary cleanup, for example:

```
Migration Import Assistant v1.0
SOURCEfire, inc.
=====
Validating backup.....OK
Collecting data from backup...
(This may take a few minutes)
Removing old sensor file sensor_interface_001E672061D8.json
```

**Step 5** Continue with [Reviewing the Manifest of Exported Configurations](#).

## Reviewing the Manifest of Exported Configurations

After the SEU/rule update equivalence check passes (or if you forced a skip of the check), the script further analyzes the package and displays a Version 4.10.3 configuration manifest:

```
4.10.3.5 Configuration Manifest
Use the arrow keys to navigate this view. Press 'q' when finished.
=====
```

This manifest is a detailed list of the Version 4.10.3 configurations that the script will either directly import or use to create new Version 5.2 configurations:

- If you exported from a standalone 3D Sensor, the script lists the intrusion policies and local rules that were applied at export time, as well as which IPS detection engines they were applied to.
- If you exported from a Defense Center, the script lists the applied intrusion policies, rules, and detection engines for all sensors managed by that Defense Center. In addition, it also lists any RNA detection engine and policy information, interface sets associated with PEP rules, compliance policies, compliance rules, and traffic profiles.

For more information on which Version 4.10.3 configurations you can migrate to Version 5.2, see [Understanding Migrated Configurations and Events, page 5-1](#).

The manifest is displayed using the `less` utility. Use the arrow keys and space bar to scroll through the manifest, then press `q` when you are done. Then, continue with [Verifying Configuration Incompatibilities, page 4-9](#).

## Verifying Configuration Incompatibilities

After you review the manifest, the script then displays a list of any Version 4.10.3 configurations in the package that will not be imported onto the Version 5.2 Defense Center. These are some of the same issues that were identified by the export script. For information on each of the issues that the configuration import script cannot resolve, see the following sections:

- [Errors Due to Unavailable Policies, page 3-9](#)
- [RNA Port Exclusion Issues, page 3-10](#)

- [Unsupported Conditions in Compliance Rules and Traffic Profiles, page 3-11](#)

If you planned correctly, the only issues listed should be those that you decided not to correct, because either you want to recreate the configurations in Version 5.2, or you do not want to migrate those configurations.

If the script identifies any unanticipated issues, Cisco recommends that you exit and resolve all critical incompatibilities, then restart the migration process. If you cannot or do not want to restart the process, you should have a thorough understanding of which configurations will not be migrated and why, so that you can recreate them later if necessary.

If the script finds issues, you must confirm your intent to continue the import:

```
Do you wish to continue with the migration? (y/n) [Y]:
```

The default is to continue. Unless you exit the migration, continue with the next section, [Resolving Configuration Conflicts, page 4-10](#).

## Resolving Configuration Conflicts

After you review the configurations that will not be migrated, the script gives you an opportunity to resolve additional issues. These are some more of the issues that were identified by the export script and discussed in [Addressing Configuration Incompatibilities, page 3-7](#). If you planned correctly, the only issues listed by the import script at this point should be those you decided to resolve during import.

For more information on each of the conflicts that the script can prompt you to resolve, see the following sections:

- [Assigning One Detection Engine of Each Type to Interface Sets, page 4-10](#)
- [Creating Intrusion Policies For Custom Detection Engine Variables, page 4-11](#)
- [Adding Service Metadata to Intrusion Rules, page 4-11](#)
- [Resolving Unsupported RNA and RUA Fast-Path PEP Rules, page 4-12](#)
- [Limiting Access Control Rules Associated with RNA Port Exclusions, page 4-13](#)

## Assigning One Detection Engine of Each Type to Interface Sets

In Version 4.10.3, you could monitor one interface set with multiple IPS (or RNA or RUA) detection engines. This would allow you, for example, to analyze the same traffic with multiple intrusion policies.

Version 5.2 does not support this capability. Now, you apply one access control policy to a device. In that access control policy, if traffic matches an access control rule you can analyze it with one intrusion policy; if it matches no rules, you can analyze it with a different intrusion policy (the default action policy).

If you exported Version 4.10.3 configurations where more than one IPS or RNA detection engine monitored the same interface, the script prompts you to choose one, for example:

```
Multiple ids detection engines are using interface set 'passive_interfaces' from
Sensor_B.
Please select the detection engine to use for 'passive interfaces':
1: Default IPS Detection Engine (Sensor_B)
2: Second IPS Detection Engine (Sensor_B)
Enter a number [1]:
```

Choosing a detection engine in this case associates the intrusion policy that was applied to that detection engine in Version 4.10.3 with a rule in the new Version 5.2 access control policy. This access control rule is configured so that it analyzes the traffic in a security zone that you will later create. The default is the first option.migrate

Choosing an RNA detection engine uses the RNA detection policy that was applied to that detection engine as a basis for your Version 5.2 discovery and logging configurations.

Although it is unlikely that you were using more than one RUA detection engine to monitor the same traffic (because there was no advantage to doing so), the script automatically chooses just one of them to use for Version 5.2.

## Creating Intrusion Policies For Custom Detection Engine Variables

In the Sourcefire 3D System, a variable is a representation of a port or network value that is commonly used in intrusion rules. Rather than hard-coding these values in multiple rules, to tailor a rule to accurately reflect your network environment, you can change the variable value.

In Version 4.10.3 you could configure custom variables for IPS detection engines, which had priority over intrusion policy-specific variables which, in turn, had priority over system variables. With Version 5.2, you no longer explicitly configure detection engines or detection engine variables; you still can configure policy-specific variables, which still have priority over system variables. However, this means that you cannot cleanly migrate a Version 4.10.3 intrusion policy applied to IPS detection engines that use custom variables.

To replicate Version 4.10.3 functionality and migrate custom detection engine variables, the import script can create a copy of the intrusion policy for each detection engine that used custom variables. These copies use the original intrusion policy as the base policy; each one has different policy-specific variables that correspond to one of the Version 4.10.3 custom variable sets.

Because this can result in a proliferation of intrusion policies, the import script prompts you whether to create the copies, for example:

```
Intrusion Policies with customized variable definitions must be created in order to
accurately migrate Detection Engine variables. These policies will use the Intrusion
Policy that is applied to the Detection Engine as the base policy.
Policy_A (copy for variables from 'DE_Alpha')
Policy_B (copy for variables from 'DE_Beta')
Do you want to create these policies? (y/n) [y]:
```

The default is to create the copies. If you decline, the script does not migrate custom detection engine variables and your Version 5.2 configurations will use only the parent intrusion policy.

## Adding Service Metadata to Intrusion Rules

In Version 4.10.3, local intrusion rules that inspect traffic only on specified ports do so regardless of the application detected in the traffic. In Version 5.2, for an intrusion rule to inspect application traffic, that rule **must** include a service metadata option for the identified application.

The import script identifies local intrusion rules that have port constraints but no corresponding service metadata, and generates one or more service metadata recommendations based on the rule content. Then, the script prompts you to accept, review, or reject the recommendations, for example:

```
3 Intrusion rules were found that may require service metadata options in order to
function properly in 5.2.0.
Do you want to review the suggestions, accept all suggestions, or skip adding service
metadata? (accept/review/skip) [accept]:
```

The default is to accept all recommendations.

If you choose to *review* recommendations, the script displays each service metadata-rule combination recommendation individually, which you can accept or reject, for example:

```
Rule: 1:1000000 "http-all"
Source port: any
Destination port: 80
```

```
Protocol: tcp
Service recommendations: http
Add 'service http' metadata? (y/n) [y]:
```

If there is one metadata recommendation for a rule, the script prompts you once; if there are eight applications that commonly use that port, the script prompts you eight times. While reviewing, the default is to accept each recommendation.

Note that you **cannot** use the script to add more than eight service metadata entries; the script presents the first eight, alphabetically. You can add additional metadata after the migration.

If you have a large number of local rules to import, you can also `skip` adding service metadata rather than reviewing each rule individually.


**Note**

Skipping the addition of service metadata will stop the affected intrusion rules from firing until you add service metadata after the migration. For more information, see the *Understanding and Writing Intrusion Rules* chapter in the *Version 5.2 Sourcefire 3D System User Guide*.

Note that the script does not allow you to review or automatically add service metadata to local intrusion rules that inspect traffic basic on port negations. For these rules to fire, you **must** manually add service metadata after the migration. The script warns you which rules need this manual update, for example:

```
The following Intrusion rules contain port negations and cannot be automatically
updated. These rules may require service metadata options to be added manually after
migration is complete:
1:1000001 "port_negation_rule"
```

## Resolving Unsupported RNA and RUA Fast-Path PEP Rules

The import script migrates Version 4.10.3 PEP rules with an action of **Fast Path** by creating access control rules that trust the specified traffic. For information on how other types of PEP rule are migrated, see [Migrating PEP Rules into Access Control Rules, page 5-3](#).

Because of the way Version 5.2 access control rules handle traffic, you cannot have traffic bypass discovery (RNA or RUA) but still be analyzed by an intrusion policy (IPS). Therefore, Version 4.10.3 RNA and RUA fast-path PEP rules **cannot** be migrated unless you also fast-path IPS.

The import script warns you of these rules, for example:

```
A PEP rule applied to 'passive interfaces' has an action of 'DE-specific' and is set
to fast path IPS and RNA. This rule cannot be migrated as-is to 5.2.0:
FASTPATH ips, rna 0.0.0.0/0 > 0.0.0.0/0 vlan: 122
Delete, fast path only IPS, or fast path all traffic? (del/ips/all) [del]: del
```

You have three choices:

- If you delete (`del`) the configuration, the default, the traffic associated with the Version 4.10.3 PEP rule will be subject to analysis by the new access control policy. The system will **not** trust, or fast path, any of that traffic.
- If you fast path only IPS traffic (`ips`), the script creates an access control rule for with an action of **Allow**, but no associated intrusion policy, to inspect matching traffic. This permits traffic to be inspected by discovery, but not an intrusion policy.
- If you fast path `all` traffic, the script creates an access control rule with an action of **Trust** for matching traffic. This allows traffic to pass without further inspection.

## Limiting Access Control Rules Associated with RNA Port Exclusions

In Version 4.10.3, you configured host discovery and flow data logging in RNA detection policies, and could easily exclude a port associated with a specific IP address from having its sessions logged.

In Version 5.2, logging and monitoring functionality is split: the access control policy governs which connections (flows) are logged on a per-access-control-rule basis, but the network discovery policy governs host discovery. Access control rules also define the traffic that you allow, and only traffic that you allow (as opposed to outright block or trust) can be monitored with discovery or subject to an intrusion policy.

To exclude traffic to and from a specific host from connection logging while preserving logging and inspection for other hosts, the script must create multiple access control rules for combinations of intrusion inspection and port exclusion preference; see [Migrating RNA Settings into Rules and Logging Preferences, page 5-7](#).

If your Version 4.10.3 RNA detection policies specified **Source/Destination** ports to exclude, the configuration import script prompts you to choose whether to create these extra rules in the new access control policy, for example:

```
There are 2 "Ports to Exclude" entries in applied RNA detection policies. Creating
access control rules to avoid logging sessions on these ports can significantly
increase the complexity of the new access control policy.
Do you want to create these extra rules? (y/n) [n]:
```

To avoid a confusing proliferation of rules, the default option is to create the access control policy without them.

**Note**

You cannot migrate source-only or destination port exclusions at all.

## Creating Security Zones Based on Interface Sets

The Version 4.10.3 concept of interface sets is replaced by Version 5.2 *security zones*, which are groupings of one or more interfaces that you can use to manage and classify traffic flow in various policies and configurations. The interfaces in a single zone may span multiple devices; you can also configure multiple zones on a single device. Using zones allows you to divide the network into segments where you can apply various policies. You must assign at least one interface to a security zone to match traffic against that security zone, and each interface can belong to only one zone. Note that the sensor migration script automatically assigns migrated passive interfaces, but not inline or inline with failopen interfaces, to security zones. See [Completing Your Version 5.2 Deployment, page 4-33](#).

**Tip**

In Version 5.2, an *inline set* refers to one or more pairs of inline interfaces that you group to streamline the applying of various networking settings. Inline sets are unrelated to security zones; not all the ingress interfaces in an inline set must belong to the same zone.

In addition to using security zones to group interfaces, you can use zones in various places in the system's web interface, including access control policies, network discovery rules, and event searches. For example, you could write an access control rule that applies only to a specific source or destination zone, or restrict network discovery to traffic to or from a specific zone.

For each active Version 4.10.3 detection engine in the package you are importing (detection engines that do not have a policy applied are not migrated), the configuration import script prompts you to create a security zone on the Defense Center. Later, after you add your migrated Version 5.2 devices to the Defense Center, you can assign their interfaces to these zones.

**Note**

Although the import script can create security zones, you must **manually** assign the interfaces on migrated Version 5.2 devices to those zones if you want to match traffic against those zones. Note that the sensor migration script automatically assigns passive, but not inline or inline with failopen, interfaces to zones. For more information, see [Configuring and Verifying Sensing Interfaces and Inline Sets](#), page 4-33.

For example, consider the following scenario:

- you are importing a configuration package onto a 5.2.0 Defense Center that has an existing security zone named *passive\_zone*, which groups interfaces that you want to monitor passively
- the package was exported from a Version 4.10.3 Defense Center that managed two Version 4.10.3 sensors: Sensor\_A and Sensor\_B
- Sensor\_A had a detection engine that monitored an inline-with-failopen interface set named *failopen\_interfaces*
- Sensor\_B had a detection engine that monitored a passive interface set named *passive\_interfaces*

First, the script prompts you to select a security zone for the failopen\_interfaces set on Sensor\_A:

```
Security Zone Creation
=====
Which security zone should be used for interface set 'failopen_interfaces' from the
sensor 'Sensor_A'?
1: passive_zone (passive)
Enter a number or a new zone name [failopen_interfaces]:
```

Accepting the default option creates a new zone that shares the name of the migrated detection engine—in this case, *failopen\_interfaces*. You can also type a different name at the prompt.

The import configuration script then prompts you to select a zone for the interfaces in the passive\_interfaces set on Sensor\_B. Notice how the zone you just created appears in the list:

```
Which security zone should be used for interface set 'passive_interfaces' from the
sensor 'Sensor_B'?
1: failopen_interfaces (inline)
2: passive_zone (passive)
Enter a number or a new zone name [passive_interfaces]: 2
```

In this example, you could type 2 (or *passive\_zone*) and press Enter. In this case, the script will not create a new security zone on the Defense Center.

**Tip**

When configuring a migrated device's interfaces and inline sets, you are **not** required to assign all the interfaces in an inline set to zones created by the import script, although you may want to for the initial configuration and policy apply steps. Zones are meant to group multiple interfaces for security purposes; in practice you might, for example, group all ingress interfaces in the same zone regardless of their inline set. For more information on how interfaces, inline sets, and zones interact in Version 5.2, see the *Sourcefire 3D System User Guide*.

After you select or create security zones for your Version 5.2 deployment, continue with [Providing Basic Access Control Settings](#), page 4-15.

## Providing Basic Access Control Settings

Access control is a new policy-based feature that allows you to specify, inspect, and log the traffic that can traverse your network. An *access control policy* determines how the system handles traffic on your network, including which intrusion policies are used and when. Because access control policies define the traffic that you permit, they also define the traffic you can monitor with the discovery feature (previously *RNA* and *RUA*).

### Naming the Policy

The script prompts you to choose a name for the new policy, for example:

```
Access Control Policy Creation
=====
In 5.2, the access control policy allows you to specify, inspect, and log the traffic
that can traverse your network. To migrate IPS, RNA, and PEP configurations, an access
control policy must be created. What do you want to call this policy?
Enter a name [Migration from My_4.10.3_Defense_Center]:
```

Accepting the default option creates a new policy named after the appliance that exported the configuration package. You can also type a different name at the prompt.



Tip

Do **not** create an access control policy with the same name as an existing access control policy on the Defense Center, because this can be confusing. If you are re-importing configurations from an appliance, accepting the default name offered by the script automatically creates a second, identically named access control policy. Therefore, Cisco recommends that you delete the older policy or choose a different name when re-importing configurations. For more information, see [Re-Importing Configurations from the Same Appliance, page 4-18](#).

### Associating an Intrusion Policy with the Default Action

In Version 5.2, the access control policy's *default action* specifies how the system handles traffic that does not meet the conditions of any access control rule in an access control policy.

The script prompts you to select an intrusion policy to associate with the default action and thus use to inspect all default-action traffic. You can choose any intrusion policy that exists on the Version 5.2 Defense Center, or you can choose one from the configuration package you are importing. The script lists both system -provided and user-created policies, for example:

```
The default action of the access control policy determines how to handle traffic that
does not match any rule in the policy. What intrusion policy do you want to use to
inspect traffic handled by the default action?
Sourcefire authored policies
1: Balanced Security and Connectivity
2: Connectivity Over Security
3: Experimental Policy 1
4: Network Discovery Only
5: Security Over Connectivity
User created policies
6: Initial Inline Policy My_4.10.3_Defense_Center
7: Initial Passive Policy My_4.10.3_Defense_Center
Enter a number [1]:
```

The default is to associate the system-provided *Balanced Security and Connectivity* intrusion policy with the default action. You can specify a different policy by typing its name or number at the prompt.

Note that choosing option 4: *Network Discovery Only* creates a default action that is **not** associated with an intrusion policy at all, but that allows all default-action traffic to be inspected by network discovery. This is useful in discovery-only (RNA-only) deployments.

**Caution**

Do **not** use Experimental Policy 1 unless instructed to do so by a Cisco representative. Cisco uses this policy for testing.

After you provide basic access control settings, continue with [Verifying the Migrated Configuration](#).

## Verifying the Migrated Configuration

As a final step, the script displays what the results of the migration will be if you continue with the import. It lists:

- the security zones that the script will create or modify
- any intrusion policies and local intrusion rules the script will import
- the access control policy the script will create, including a detailed list of the access control rules in the policy and their associated conditions, actions, and intrusion policies
- any rules that the script will add to the network discovery policy, and their associated networks-to-monitor and other discovery options
- any correlation policies, correlation rules, and traffic profiles that the script will import and activate

Although not listed by the script, the import script will also update various discovery-related settings in the system policy and network discovery policy on the Version 5.2 Defense Center. For details on how your Version 4.10.3 configurations translate to Version 5.2, and for information on the new configurations that the migration process creates, see [Understanding Migrated Configurations and Events](#), page 5-1.

The script displays the migrated configuration using the `less` utility. Use the arrow keys and space bar to scroll through the configuration, then press `q` when you are done. Continue with [Confirming the Import and Resolving Configuration Collisions](#), page 4-16.

## Confirming the Import and Resolving Configuration Collisions

After you review the proposed results of the migration, the import script asks you whether you want to proceed:

```
Are you sure you want to import this backup? (y/n) [y]:
```

If you exit the script at this point no changes are made to the Version 5.2 Defense Center, except the cleanup of various files from any previous migrations. If you continue, which is the default, the script begins to import the configurations in the package to the Defense Center.

At this point, if a configuration in the package directly conflicts with an existing configuration on the Defense Center, the script prompts you to resolve the conflict.

This occurs because certain configurations, sometimes called objects, are uniquely identified by the system. Multiple versions of the same object cannot exist on a Defense Center. For example, the script might display the following prompt for a conflicting intrusion policy:

```
The object My_Intrusion_Policy (IntrusionPolicy) already exists. Overwrite? (y/n/all) [y]:
```

The script displays similar prompts for conflicting local intrusion rules, correlation policies and rules, and traffic profiles. The default is to overwrite the older configuration with the one in the package you are importing. You can also keep the older configuration, or specify `all` to overwrite all remaining conflicting configurations.



Tip

This type of conflict occurs only if you are re-importing configurations. For more information on why configurations conflict and what you can do to prevent collisions, see [Re-Importing Configurations from the Same Appliance](#), page 4-18.

After you resolve any object conflicts, the script saves the new configurations to the Version 5.2 Defense Center. The script also activates any correlation policies and traffic profiles that were active in your Version 4.10.3 deployment:

```
Writing configuration.....
Activating 0 correlation policies and 1 traffic profiles...
```

You can now log out of the Defense Center and continue with the next step in your migration plan. Depending on your deployment, it may be time to perform additional configuration imports, or import events, or reimaged your Version 4.10.3 3D Sensors into Version 5.2 devices. For more information on planning your migration, see [Understanding the Migration Process](#), page 2-1.

## Configuration Import Script Syntax and Options

You must run the configuration import script as the root user. Cisco recommends that you copy the configuration package to the migration directory (`/var/sf/migration`) and run the script from that directory using `sudo`, providing your password when prompted.

After you log in to the appliance's shell as an Administrator (see [Logging Into an Appliance to Run Migration Scripts](#), page 4-2), the syntax for running the script is as follows:

```
sudo ./config_import.pl exported_config_package.tgz options
```

where `exported_config_package.tgz` is the package you copied to the Defense Center and `options` represents one or more script options, as described in the table below. Note that if you are not running the script from the migration directory, or you did not copy the package to the migration directory, make sure you provide relative or absolute paths to the script and package.

**Table 4-5** Configuration Import Script Options

| Option     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| none       | Performs the import beginning with the SEU/rule update equivalence check, as described in <a href="#">Starting the Configuration Import Script</a> , page 4-8.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| --manifest | Display a detailed list of the Version 4.10.3 configurations in the specified package. If a review of the manifest reveals anything unexpected, Cisco recommends that you fix critical issues and export a new package from the Version 4.10.3 appliance. For more information, see <a href="#">Reviewing the Manifest of Exported Configurations</a> , page 4-9.                                                                                                                                                                                                                                                 |
| --force    | Forces the script to skip the SEU/rule update equivalence check.<br><br>Do <b>not</b> use this option unless you have already reimaged the appliance where you exported the package. Otherwise, Cisco recommends that you update the SEUs and rule updates in your deployment and restart the migration process; for more information see <a href="#">SEU and Intrusion Rule Update Requirements</a> , page 3-3.<br><br>In most cases, the resulting imported intrusion configurations will work as expected. However, contact Support if you cannot edit or apply policies after forcing a configuration import. |

Table 4-5 Configuration Import Script Options (continued)

| Option        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --usedefaults | Run the script without providing any user input, using the default answer for all prompts, including conflict resolution, security zone creation, and access control policy settings. See the previous sections for more information on the default choices the import script makes.<br><br>Do <b>not</b> use this option unless you fully understand which Version 4.10.3 configurations will be migrated and what the resulting Version 5.2 configurations will be. |
| --help        | Display basic instructions and syntax for running the script.                                                                                                                                                                                                                                                                                                                                                                                                         |

## Importing Configurations Multiple Times

In a properly planned migration, you run the import script once for each configuration package you need to migrate to Version 5.2. For example, in a simple single Defense Center-to-single Defense Center migration, you would run the configuration import script only once during the whole migration process. However, there are a few situations where you must run the configuration import script more than once.

### Importing Multiple Unique Configuration Packages

If you are replacing two or more Version 4.10.3 Defense Centers with one Version 5.2 Defense Center, or if you are adding several former standalone 3D Sensors to a new Defense Center, you must import multiple unique configuration packages onto the Version 5.2 Defense Center.

Running the import script cleans up information from any previous invocations. Also, although the sensor migration script copies and applies interface configurations, importing configurations with the import script **does not** configure interfaces to reimaged Version 5.2 devices. Therefore, when you have multiple unique packages to import, and you do not intend to use the sensor migration script to migrate some or all sensors, you should run the display interfaces script **immediately** after each import, and save that script's output to a file that will not be overwritten. In cases where you do not use the sensor migration script, this preserves the information on how to configure the interfaces on the migrated devices associated with each package after you add the devices to the Defense Center. Alternately, add and configure all devices referenced in the imported package before you perform the next import.

For information on using the display interfaces script, see [Configuring and Verifying Sensing Interfaces and Inline Sets, page 4-33](#).

### Re-Importing Configurations from the Same Appliance

If you have planned your migration correctly, you should only run the configuration import script one time for each exported configuration package. However, you may decide that the results of your migration are not what you want, and that your issues can be resolved by another import.

You can either:

- re-import the same package but choose different options during import, or
- re-import a different package.

For example, if the Version 4.10.3 appliances whose configurations you are migrating have not already been reimaged, you can update those configurations then create a new package for re-import.

In either case, there are consequences to a re-import that can affect the migrated configurations on the Defense Center, as described in the following list.

### security zones

For each active Version 4.10.3 detection engine in the package you are importing (detection engines that do not have a policy applied are not migrated), the script prompts you to choose or create a security zone on the Defense Center. Later, after you add your migrated Version 5.2 devices to the Defense Center, you can assign their interfaces to these zones.

In a package re-import, Cisco recommends that you choose the same zones you created in the first import. If you did not rename any interface sets in the Version 4.10.3 deployment before you re-exported, accepting the default answers, no new security zones will be created. However, if you changed the name of an interface set in the exported package, accepting the script defaults can create a new zone.

### access control policy

Every time you run the import script, the script creates a **new** access control policy. If you are re-importing configurations, accepting the default name offered by the script automatically creates a second, identically named access control policy.

Because it is confusing to have two policies with the same name, Cisco recommends that you delete the older policy before you begin the import, or choose a different name on re-import.

### unique configurations (objects)

The system uniquely identifies the following migrated configurations, sometimes called objects:

- intrusion policies and local intrusion rules
- correlation policies and rules
- traffic profiles

Multiple versions of the same object **cannot** exist on a Defense Center. If you import a package that contains an object that already exists on the Version 5.2 Defense Center, you must choose which to keep: the existing object or the object in the package. Note that this conflict occurs even if either object has been renamed or otherwise modified.

As an example, consider a scenario where you import a configuration package onto a Version 5.2 Defense Center, then decide that the results are not what you want. You return to your Version 4.10.3 deployment, modify some configurations, then export an updated package. When you import that updated package onto the Version 5.2 Defense Center, all intrusion policies and local intrusion rules, correlation policies and rules, and traffic profiles that were imported the first time and that still exist on the Defense Center now conflict with their counterparts in the updated package.

For your convenience, the import script prompts you to make a decision for each conflicting object; the default is to overwrite the existing configuration with the one from the configuration package. For more information, see [Confirming the Import and Resolving Configuration Collisions, page 4-16](#).

**Tip**

To avoid object collision, before you begin a configuration re-import delete any existing objects that will conflict.

### network discovery policy, rules, and other discovery settings

The import script translates some of the RNA network monitoring settings in your Version 4.10.3 deployment to Version 5.2 discovery rules in the network discovery policy.

Because there is only one network discovery policy on a Version 5.2 Defense Center, the script merges (instead of overwrites) the network monitoring settings on the Defense Center with those in the import package. This could result in duplicate discovery rules. Therefore, Cisco recommends that you delete any network discovery rules created by the first import before you begin the re-import.

In addition, a re-import can overwrite other settings in the network discovery policy.

## Importing Events onto a Version 5.2 Defense Center

**Supported Devices:** None

**Supported Defense Centers:** Any

As an optional and usually one of the final steps in a migration process, you can import the intrusion and audit events that you exported from your Version 4.10.3 appliances.

First, copy a Version 4.10.3 event package (see [Exporting Events from a Version 4.10.3 Appliance, page 4-6](#)) to the appropriate Version 5.2 Defense Center. Then, run a script that imports the events. You should run the import script once for each event package you need to import:

- If you are migrating from a single Version 4.10.3 Defense Center to a single Version 5.2 Defense Center, you should only have one event package to import.
- If you are replacing two or more Version 4.10.3 Defense Centers with one Version 5.2 Defense Center, or are adding several former standalone 3D Sensors to a new Defense Center, you must import each event package individually.

When you run the script, it warns you if you do not have enough disk space on the Defense Center to import the events in the package. Do **not** proceed if there is not enough disk space for the import; the import will fail. Before you try again, free space on the appliance by deleting extraneous events, saved backup files, and so on.

Note that some fields in intrusion events generated by Version 4.10.3 are different from the fields in Version 5.2 intrusion events. For information on how legacy events appear in the Version 5.2 web interface, see [Understanding Migrated Intrusion and Audit Events, page 5-18](#).

Also, the timestamps on migrated events will be “behind” newly generated events on the Version 5.2 Defense Center. Because the database is pruned by event timestamp, your migrated events will be pruned before those events.

Finally, keep in mind that importing events can take a significant amount of time.



### Tip

If imported events do not display after you complete the import process, clear your browser cache and try again.

### To import a package of intrusion and audit events:

**Access:** Admin

- 
- Step 1** Copy the package you plan to import to the Version 5.2 Defense Center.  
Cisco recommends that you copy all packages to the `/var/sf/migration` directory.
- Step 2** Log into the Defense Center’s shell using an account with Administrator privileges.  
For more information, see [Logging Into an Appliance to Run Migration Scripts, page 4-2](#).

**Step 3** Navigate to the migration folder:

```
cd /var/sf/migration
```

**Step 4** Run the export script as the root user, providing your password when prompted:

```
sudo ./event_import.pl exported_event_package.tgz
```

where *exported\_config\_package.tgz* is the package you copied to the Defense Center. If you did not copy the package to the migration directory, make sure you provide a relative or absolute path to the package.

After you provide your password, the script starts. It compares the disk space required to complete the import with the space available on the Defense Center and asks if you want to proceed, for example:

```
Migration Event Import Assistant v1.0
SOURCEfire, inc.
=====
Validating backup...
Importing these events will take approximately 125MB.
There is approximately 15G free.
Are you sure you want to import this backup? (y/n) [y]: y
```

**Step 5** Choose whether you want to proceed by typing *y* or *n* and pressing Enter.

Do **not** proceed if there is not enough disk space for the import; the import will fail. Before you try again, free space on the appliance by deleting extraneous events, saved backup files, and so on. If you confirm that you want to proceed, the script begins importing the events:

```
Importing events...
Migration event import complete!
```

**Step 6** Continue with the next step in your migration plan.

For more information on planning your migration, see [Understanding the Migration Process, page 2-1](#).

## Rebuilding Version 4.10.3 Appliances

As part of the migration to Version 5.2, you must either replace, reimagine, or re-create your Version 4.10.3 appliances. The method and timing depend on the type of appliances in your deployment and on your migration plan.

If you are **replacing** a physical appliance or **re-creating** a virtual appliance, perform the initial setup on the new Version 5.2 appliance and prepare it for configuration import **before** you take its Version 4.10.3 counterpart out of band or begin running any migration scripts. After you set up the new Version 5.2 appliance, you can add it to your deployment seamlessly at the time determined by your migration plan.

If you are **reimagining** a physical appliance **during** the migration, your migration plan must account for the time it will take to perform the reimage. Because reimaging results in the loss of almost **all** configuration and event data on the appliance, including special configurations such as LDAP authentication, your plan must also account for setup and import preparation.

To reimage sensors, you can install the sensor migration script on the Version 5.2 Defense Center and remotely reimage one or more standalone or managed Series 2 or Series 3 3D Sensors. The script automatically copies the sensors' interface configurations, reimages the sensors, registers the reimaged sensors to the Defense Center, and applies the interface configurations.



### Caution

Contact Support before using the sensor migration script to migrate a 3D500 3D Sensor.

You must manually reimage Version 4.10.3 Defense Centers to Version 5.2. In some cases (for example, in a small or low-bandwidth deployment) you might also prefer to manually reimage Series 2 and Series 3 3D Sensors.

When you replace or manually reimage a physical sensor, or re-create a virtual sensor, you must also manually add it to the Version 5.2 Defense Center and configure its interfaces.

**Caution**

Make sure you allow sufficient time for the restore process to complete. If you interrupt the process (for example, by pressing Ctrl + C or rebooting), you could cause an unrecoverable error. If you think the restore is taking too long or you experience any other issues with the process, **do not** quit, reboot, or otherwise interrupt the process. Instead, contact Support. For more information, see [CAUTION: Do Not Interrupt the Reimage Process, page 2-2](#).

Use the following resources to complete appliance replacements, re-creations, or manual reimages:

- See the appropriate *Version 5.2 Installation Guide* for instructions on replacing, recreating, and manually reimaging appliances,
- See [Understanding the Migration Process, page 2-1](#) for information on:
  - migration- and deployment-specific information on manual reimaging
  - reimaging using the sensor migration script
  - replacing and recreating appliances
  - details on when or whether to take Version 4.10.3 appliances out of band
  - when to start using Version 5.2 appliances
- See [Preparing for Migration, page 3-1](#) for migration-specific information on preparing a new or freshly reimaged Version 5.2 Defense Center or standalone sensor for configuration import, including:
  - intrusion rule update requirements
  - license requirements
  - instructions for installing the migration script

Additionally, see the following sections for more information on using the sensor migration script and manually adding devices:

- [Reimaging and Registering Devices with the Sensor Migration Script](#).
- [Manually Adding Version 5.2 Devices to the Defense Center, page 4-31](#).

## Reimaging and Registering Devices with the Sensor Migration Script

**Supported Devices:** Series 2, Series 3

You can use the sensor migration script to remotely reimage one or more Version 4.10.3 (or a later patch) 3D Sensors to Version 5.2. First, you install the script on your Version 5.2.0.x Defense Center using the Defense Center's web interface. Then you run the script as the root user from the Defense Center's shell, typically via SSH. Alternately, you can also connect to the Series 3 Defense Center shell via Lights-Out Management (LOM). Status messages display migration progress.

**Caution**

Contact Support before using the sensor migration script to migrate a 3D500 3D Sensor.

You install one of two script packages depending on whether you run the script from a Series 2 or Series 3 Defense Center. See [Table 3-4 on page 3-12](#) for more information. The script from either package can reimage multiple Series 2 and Series 3 sensors in parallel.

You **cannot** use the script to migrate virtual devices. You **can** use the script to migrate any eligible physical sensor on your network, regardless of whether you first import configurations or events. The script copies your Version 4.10.3 sensor interface configurations to the Defense Center, reimages the sensors, registers the sensors to the Version 5.2.0.x Defense Center where you run the script, and applies the interface configurations. During the migration, sensor interfaces that were configured to fail open remain open, allowing network traffic to pass without interruption.

**Note**

Inline interfaces **fail closed** during the reimage when you do not use the sensor migration script, or you use the script and the interfaces are not configured to fail open. In these cases, you may want to remove the sensors from your critical network path during reimage, which may require physical access to the sensors.

The script automatically reboots reimaged sensors at the appropriate migration stage. As a precautionary measure, it disables the use of Ctrl+C when you have responded to all prompts and the migration process begins.

**Caution**

**Do not** interrupt the migration or reboot your 3D Sensors or Defense Center during the sensor migration. This could corrupt the rebooted system or negatively affect migrated configurations.

You can run the script multiple times. For example, you might want to test the migration on a few sample sensors before migrating remaining sensors, or migrate sensors in groups to avoid performance issues. If a sensor fails to migrate, the script skips the failed sensor and continues migrating the other sensors. If you migrate a single sensor and it fails, or you migrate multiple sensors and all sensors fail, the script aborts. In most cases, you can include failed sensors in a subsequent migration.

Although you can migrate up to twenty sensors at a time, Cisco recommends for performance reasons that you migrate no more than ten sensors at a time. The script cautions you before you add another sensor when you have already added ten or more sensors.

Reimaging results in the loss of almost **all** configuration and event data on the sensor. Although reimaging can retain the sensor's network, console, and Series 3 Lights-Out Management (LOM) settings, and the sensor migration script can register sensors and preserve interface configurations, you must perform all other setup tasks after the restore process completes. See [Completing Your Version 5.2 Deployment, page 4-33](#) for more information.

In the event of an unavoidable migration interruption such as a power outage, you can manually reimage interrupted sensors to Version 5.2 in most cases. However, you lose the script's advantages of allowing sensors to fail open, copying interface configurations, registering sensors, and providing remote access. If the interruption occurs at a critical stage of the migration and you to lose access to the sensor, contact Support. For instructions on manually reimaging a sensor, see the appropriate *Version 5.2 Installation Guide*.

**Tip**

You can run the sensor migration script from a Version 5.3 Defense Center if you update the Defense Center from Version 5.2.0.x after installing the script. You cannot install the script directly on a Version 5.3 Defense Center. For example, if you want to manage Version 5.3 devices while migrating sensors, you must install the sensor migration package on your Version 5.2.0.x Defense Center before updating it to Version 5.3.

Note that a Version 4.10.3.x Defense Center where a migrated sensor was originally registered still shows configured interfaces and detection engines for the sensor after the migration; these non-functional *ghost images* are merely artifacts of the migration.

See the following sections for more information:

- [Running the Sensor Migration Script, page 4-24](#)
- [Understanding the Status Display, page 4-27](#)
- [Understanding End-of-Run Error Messages, page 4-29](#)
- [Resolving SSH Key Conflicts, page 4-31](#)

## Running the Sensor Migration Script

After you import and install the sensor migration package using the Version 5.2.0.x Defense Center web interface, run the script from the Defense Center command line as the root user. The script prompts you for the following information:

- the user name and password of an account with `sudo` privileges on the Version 5.2 Defense Center where you run the script.

The script typically pauses approximately three minutes to verify this account information, and aborts if you provide invalid information.

- the IP address or host name for each sensor you want to migrate, and a user name and password of an account with `sudo` privileges for each.

The script pauses three to five minutes to verify communication between the sensor and the Defense Center each time you provide the user name and password for a sensor; if the script must resolve invalid SSH keys, the pause can be up to approximately eight minutes. See [Resolving SSH Key Conflicts, page 4-31](#) for more information.

Cisco recommends that you use the `admin` account for the Version 5.2 Defense Center where you run the script and for each sensor you specify.



### Caution

**Do not** use an LDAP or Radius account for sensor migration. External authentication configurations are not migrated. The reimaged software could exhibit unpredictable behavior, and the script cannot register migrated sensors to the Version 5.2.0.x Defense Center.

The script uses the authentication information you provide to facilitate SSH communication over port 22 between migrating 3D Sensors and the Defense Center. If you provide an invalid sensor IP address, host name, user name, or password, the script re-prompts you.

Finally, the script lists the sensors you have identified and asks if you want to proceed. If you proceed, the script disables Ctrl+C as a precautionary measure and begins the migration.

The following table explains the options you can use with the sensor migration script.

**Table 4-6**      **Sensor Migration Script Options**

| Option                       | Description                                                                                                                                            |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--timeout=value</code> | Configures the script to run for <i>value</i> minutes before timing out, where <i>value</i> is a number greater than the default value of 120 minutes. |
| <code>--help</code>          | Describes the options you can use when running the script.                                                                                             |

**To reimage and register Version 4.10.3 Sensors:****Access:** Admin

- Step 1** Obtain the sensor migration package and install it on your Version 5.2.0.x Defense Center. See [Obtaining and Installing Migration Packages, page 3-12](#) for more informations.

**Caution**

Make sure you allow sufficient time for the restore process to complete. If you interrupt the process (for example, by pressing Ctrl + C or rebooting), you could cause an unrecoverable error. If you think the restore is taking too long or you experience any other issues with the process, **do not** quit, reboot, or otherwise interrupt the process. Instead, contact Support. For more information, see [CAUTION: Do Not Interrupt the Reimage Process, page 2-2](#).

- Step 2** Log into the Defense Center's shell using an account with `sudo` privileges.  
For more information, see [Logging Into an Appliance to Run Migration Scripts, page 4-2](#).

- Step 3** Switch to the root user and provide the password when prompted. For example:

```
sudo su
Password:
```

- Step 4** Navigate to the sensor migration directory:

```
cd /Volume/migration_tmp
```

- Step 5** Enter either of the following commands, depending on whether you want to modify the default timer setting:

- To run the script using the default timeout value of 120 minutes, enter:

```
./migration_script.pm
```

- To run the script using a different timeout value, enter:

```
./migration_script.pm --timeout=value
```

where *value* is the number of minutes (120 or greater) before the timer expires.

The script displays a welcome message, then prompts you for the Defense Center's user name and password. For example:

```
#####
#
Welcome to the Sourcefire Sensor Migration Script
#
#####
```

This script is intended to be run on a 5.2 Defense Center and will upgrade 4.10.3 devices to 5.2.

In order for migration to complete successfully, the following conditions must be met:

- \* This Defense Center must be running version 5.2 or greater
- \* The Sensors to be migrated must be running version 4.10.3 or greater
- \* Communication between Defense Center and Sensor(s) must be possible

Please also note that once the migration process is begun, it must be allowed to run to completion.

Sensors to be migrated will need to contact this Defense Center for update information. Please provide a username (with `sudo` privileges and password for this Defense Center).

```
Username:admin
Password:
```

- Step 6** Enter the user name and password for an account with `sudo` privileges on the Version 5.2 host Defense Center. Cisco recommends that you use the `admin` account.

**Caution**

**Do not** use an LDAP or Radius account for sensor migration. External authentication configurations are not migrated. The reimaged software could exhibit unpredictable behavior, and the script cannot register migrated sensors to the Version 5.2.0.x Defense Center.

These credentials facilitate communication between migrating 3D Sensors and the Defense Center. The script validates the credentials and aborts if the information is invalid:

```
Verifying credentials (this may take several minutes)... Authentication failure.
Unable to continue.
```

If the information is valid, the script prompts you for the host name or IP address of the first sensor you want to migrate:

```
Verifying credentials (this may take several minutes)... Success
Please specify name or IP address of sensor:
```

- Step 7** Enter the host name or IP address of a Series 2 or Series 3 sensor on your network. The script asks if you want to identify another sensor.

```
Specify additional sensors? (y/n) [n]:
```

- Step 8** Enter `y` to add another sensor or press `Enter` when you have added the last sensor.

When you indicate that you have added the last sensor, the script lists each sensor and prompts you for the user name and password for the first sensor you specified. For example:

```
The following devices were specified:
192.168.13.12
kilroy (192.168.13.13)
killjoy (192.168.13.14)
192.168.13.15
Please supply a username with sudo privileges
for use with system 192.168.13.12: admin
Please supply the password for user 'admin':
```

- Step 9** Enter the user name and password for a user who has `sudo` privileges for the sensor. Cisco recommends that you use the `admin` account for each sensor.

**Caution**

**Do not** use an LDAP or Radius account for sensor migration. External authentication configurations are not migrated. The reimaged software could exhibit unpredictable behavior, and the script cannot register migrated sensors to the Version 5.2.0.x Defense Center.

For each sensor you specified, the script tests the credentials and, if more sensors remain, prompts you for the next user name and password. For example.

```
Testing ssh connection to the sensor, and from the sensor back to
the Defense Center (this may take several minutes)... Success
Please supply a username with sudo privileges
for use with system 192.168.13.13: admin
```

```
Please supply the password for user 'admin':
...
```

Note that testing the SSH connection can take three to five minutes per sensor, and up to eight minutes if the script must resolve invalid SSH keys. The script reprompts if you enter invalid information.

After successfully testing the last sensor, the script warns you that reimaging permanently deletes data from all migrated sensors and asks if you want to begin the migration process.

```
Warning: Migration will reimage sensors,
 permanently deleting data on those systems.
```

```
Start the migration process for selected devices? (y/n) [n]:
```

**Step 10** Enter `y` to start the migration process and the migration timer, or press `Enter` to exit the script.

The script displays progress information during the migration. See [Understanding the Status Display, page 4-27](#).

When the migration completes or the timer expires, messages:

- provide the result of the migration for each sensor
- remind you to inspect your interface configurations
- remind you to apply your access control policy.

For example:

```
Migration script complete.

MySensor1.example.com (192.168.13.11)
 Success: Migration and registration completed successfully.
MySensor2.example.com (192.168.13.12)
 Failure: Unable to upload new data to sensor.
Please inspect interface configurations and apply policy to migrated systems.
```

See [Understanding End-of-Run Error Messages, page 4-29](#) for more information.

**Step 11** Continue with [Completing Your Version 5.2 Deployment, page 4-33](#).

## Understanding the Status Display

The sensor migration begins after you have identified the sensors to migrate, provided the requested information (see [Running the Sensor Migration Script, page 4-24](#)), and confirmed that you want to proceed with the migration. At this point the script prohibits you from using `Ctrl+C`, begins the migration process, and informs you that it is preparing status information:

```
Preparing to Display Progress...
```

The script displays updated migration progress approximately every five seconds:

```
#####
#
Sourcefire Sensor Migration Underway
#
Please do not reboot this Defense Center!
Your terminal will refresh as progress is updated
#
#####

Backup Legacy Configuration... 6 Passed
Gathering Sensor Information... 6 Passed
Uploading New Data... 5 Passed
Updating OS Components... 4 Passed, 1 Failed
Removing Legacy 4.x Code... 4 Passed
```

```

Installing New 5.x Code... 4 Passed
Convert/Restore Legacy Configuration... 4 Passed
Reboot/Update Sensors (may take 30 mins)... 4 Passed
Cleaning Up... 4 Passed
Establishing Registration... 2 Passed, 2 Failed

42:33 until timeout

```

The screen flickers with each update, adding stages as a sensor reaches each stage and incrementing the number of sensors that have passed and failed each stage. The script also displays the minutes and seconds until the timer expires. The timer starts when you respond to the final prompt and counts down from either the default time of 120 minutes or the time you configure. See [Table 4-6 on page 4-24](#) for more information.

**Caution**

You cannot use the sensor migration script to migrate sensors that were included in a previous script run where the timer expired. In most cases, you can reimage the sensors manually using the restore procedure. See the *Version 5.2 Sourcefire 3D System Installation Guide* for information on restoring your sensors. Contact Support if the timer expires and you cannot restore your sensors.

The following table explains each stage of the migration:

**Table 4-7**      **Sensor Migration Stages**

| Migration Stage                      | Description                                                                                                 |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Backup Legacy Configuration          | Collects the Version 4.10.3 sensor interface configurations                                                 |
| Gathering Sensor Information         | Collects the sensor model number, model series, and so on so the correct migration package can be assembled |
| Uploading New Data                   | Uploads sensor-specific data and packages, including RPMs, from the Defense Center to the sensor            |
| Updating OS Components               | Installs the Version 5.2 operating system on the sensor                                                     |
| Removing Legacy 4.x Code             | Uninstalls Version 4.10 RPMs on the sensor                                                                  |
| Installing New 5.x Code              | Installs Version 5.2 RPMs on the sensor                                                                     |
| Convert/Restore Legacy Configuration | Recreates interface configurations on the newly updated Version 5.2 sensor                                  |
| Reboot/Update Sensors                | Reboots the sensor and completes the update (this can take up to 30 minutes)                                |
| Cleaning Up                          | Removes unneeded data specific to the current migration process                                             |
| Establishing Registration            | Registers the migrated Version 5.2 devices to the Version 5.2 Defense Center                                |

Sensors are migrated in parallel in a forked arrangement; that is, they begin the migration simultaneously and proceed individually, each at its own pace. Counters update to identify the number of sensors that have passed or failed each stage.

## Understanding End-of-Run Error Messages

When the migration process completes, the script identifies each sensor that successfully completed the migration and displays the same completion message for each, as shown in the following example:

```
Migration script complete.

MySensor1.example.com (192.168.13.11)
 Success: Migration and registration completed successfully.
MySensor2.example.com (192.168.13.12)
 Success: Migration and registration completed successfully.
```

When a sensor fails, the script identifies the failed sensor in a single error message that indicates the reason for the failure and suggests a course of action. For example:

```
MySensor1.example.com (192.168.13.13)
 Failure: Unable to determine sensor model.
 Please confirm that the sensor specified is online and then rerun migration.
```

When a failure occurs early in the process, you can often include the failed sensor in a script rerun after addressing the reason for the failure. When a failure occurs later in the process, the script suggests (with one exception) that you contact Support. In most cases, you can manually reimage late-stage failures using the restore procedure. The exception is when the migration succeeds and registration fails, in which case the script suggests that you register the sensor manually.

If a sensor loses connectivity for any reason during the migration, the sensor does not complete the migration and the script displays at least one end-of-run error message. These messages indicate the stage that was in progress when connectivity was lost, and the suggested actions indicate whether you can include the sensor in a script rerun.

The following table describes error messages that might display after the migration process completes.

**Table 4-8** *Sensor Migration Script End-of-Run Error Messages*

| Error Message                                                                                                                                          | Description                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| ERROR: Attempt to contact <name> failed.<br>Skipping this device and attempting to continue.                                                           | The specified sensor could not be reached.                                                                                               |
| ERROR: Sensor appears to be running an unsupported version of the STIG Hotfix.<br>Please uninstall this hotfix and retry migration or contact support. | The STIG hotfix version on the specified sensor was unavailable when the migration script was developed and is untested and unsupported. |
| ERROR: SSH Host Identification key problem for Sensor <name><br>Please resolve this SSH key difference and restart migration for this sensor.          | The migration script could not automatically resolve an invalid SSH key. See <a href="#">Resolving SSH Key Conflicts</a> , page 4-31.    |
| ERROR: Unable to connect to <sensor_data>{entry}{id}.<br>Please contact support.                                                                       | The migration script proceeded beyond a point of no return and lost communication with the specified sensor.                             |
| ERROR: Unable to resolve system name <name>.<br>Please check name and rerun migration for that system.                                                 | The specified host name could not be resolved.                                                                                           |
| ERROR: Unsupported model type (Defense Center) found for system <name> (<ip>).<br>Only Sensors can be migrated using this script.                      | The host name or IP address identified a Defense Center.                                                                                 |

**Table 4-8** *Sensor Migration Script End-of-Run Error Messages*

| <b>Error Message</b>                                                                                                                                                      | <b>Description</b>                                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| <p>ERROR: Unsupported model type (Virtual System) found for system &lt;name&gt; (&lt;ip&gt;).</p> <p>Migration of Virtual Systems is not supported.</p>                   | The host name or IP address identified a virtual Defense Center.                                              |
| <p>ERROR: Unsupported software version found for Sensor &lt;name&gt;.</p> <p>All Sensors must be running version 4.10.3 or later (but less than 5.x).</p>                 | The version of the specified sensor was earlier than Version 4.10.3, or Version 5.0 or later.                 |
| <p>Failure: md5sum of uploaded package does not match expected value.</p> <p>Please verify communication between sensor and DC and then rerun migration.</p>              | The md5sum of the uploaded package did not match the expected value.                                          |
| <p>Failure: Unable to copy legacy configuration data.</p> <p>Please contact support.</p>                                                                                  | The migration script could not copy legacy configuration files.                                               |
| <p>Failure: Unable to correctly determine system architecture.</p> <p>Please contact support.</p>                                                                         | The migration script could not determine if the sensor is 32-bit or 64-bit.                                   |
| <p>Failure: Unable to delete legacy detection engine data.</p> <p>Please contact support.</p>                                                                             | The migration script could not delete Version 4.10.3 detection engine data.                                   |
| <p>Failure: Unable to determine sensor model.</p> <p>Please confirm that the sensor specified is online and then rerun migration.</p>                                     | The migration script could not determine the sensor model.                                                    |
| <p>Failure: Unable to establish registration with Defense Center.</p> <p>Migration successful. Please attempt to establish registration with Defense Center manually.</p> | The migration script could not establish management between the migrating Defense Center and migrated sensor. |
| <p>Failure: Unable to install 5.2.0 RPM packages.</p> <p>Please contact support</p>                                                                                       | The migration script could not install the Version 5.2 RPM.                                                   |
| <p>Failure: Unable to process legacy LILO configuration</p> <p>Please contact support.</p>                                                                                | The migration script could not process the LILO boot configuration.                                           |
| <p>Failure: Unable to remove migration files</p> <p>Please contact support.</p>                                                                                           | The migration script could not delete unneeded migration files during the cleanup step.                       |
| <p>Failure: Unable to scp import/export tools from DC to localhost sensor.</p> <p>Please verify communication between sensor and DC and then rerun migration.</p>         | The migration script could not transfer migration tools to the sensor.                                        |
| <p>Failure: Unable to scp legacy configuration data from sensor to localhost DC.</p> <p>Please verify communication between sensor and DC and then rerun migration.</p>   | The migration script could not transfer legacy data from the sensor being migrated to the Defense Center.     |

**Table 4-8** Sensor Migration Script End-of-Run Error Messages

| Error Message                                                                                                                | Description                                                             |
|------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Failure: Unable to uninstall 4.10.x RPM files.<br>Please contact support.                                                    | The migration script could not uninstall the Version 4.10.x code.       |
| Failure: Unable to upgrade OS packages properly.<br>Please contact support.                                                  | The migration script could not update the operating system package.     |
| Failure: Unable to upload new data to sensor.<br>Please verify communication between sensor and DC and then rerun migration. | The migration script could not upload migration RPMs and related files. |
| killing forked processes due to timeout                                                                                      | The timeout value expired before the migration completed.               |

## Resolving SSH Key Conflicts

During the migration, the sensor migration script uses SSH on port 22 to establish connections between the Defense Center and the sensors you identify. Before beginning the migration, the script verifies that it can establish these connections. When the script encounters an invalid SSH key for the targeted sensor, the script resolves the conflict by automatically backing up the `known_hosts` file to `/home/<user>/.ssh/known_hosts_<date>_<time>` and removing the line in the file that includes the invalid key.

A message at the end of the migration process notifies you when the migration script is not able to automatically resolve an SSH key conflict. See [Understanding End-of-Run Error Messages, page 4-29](#) for more information. In this case, you can resolve the conflict and include the affected sensor in a subsequent migration.

You can resolve the conflict using either or both forms of the following command from the Version 5.2 Defense Center command line:

```
ssh keygen -R IP_address
ssh keygen -R hostname
```

If you enter the command only once, you must identify the sensor in the command using the same form (IP address or host name) that you used to identify the sensor while running the sensor migration script. If you enter both forms of the command, you can use the IP address or host name to identify the sensor while running the sensor migration script.

## Manually Adding Version 5.2 Devices to the Defense Center

When you replace physical sensors, recreate virtual sensors, or manually reimagine physical sensors instead of using the sensor migration script, you must manually register the Version 5.2 devices to the Version 5.2 Defense Center. In these cases, you should register your devices after importing configurations and events so your policies and security zones are in place.

For detailed instructions on adding devices to a Defense Center, including adding devices in a NAT environment, see the *Managing Devices* chapter in the *Version 5.2 Sourcefire 3D System User Guide*.

### To add a device to a Defense Center:

**Access:** Admin/Network Admin

- Step 1** Configure the device to be managed by the Defense Center.  
You should have designated the Defense Center as the remote manager during the device's initial setup. If you did not, use a physical device's web interface (**System > Local > Registration**) or a virtual device's CLI to add the Defense Center.
- Step 2** Log into the Defense Center's web interface, then select **Devices > Device Management**.  
The Device Management page appears.
- Step 3** From the **Add** drop-down menu, select **Add Device**.  
The Add Device pop-up window appears.

**Add Device** ? X

Host:

Registration Key:

Group:  ▼

Access Control Policy:  ▼

**Licensing**

Protection:

Control:

Malware:

URL Filtering:

VPN:

▼ **Advanced**

Host or NAT ID is required. Register Cancel

372703

- Step 4** In the **Host** field, type the IP address or the hostname of the device you want to add.  
The hostname of the device is the fully qualified domain name or the name that resolves through the local DNS to a valid IP address.



**Caution** Use a hostname rather than an IP address if your network uses DHCP to assign IP addresses.

- Step 5** In the **Registration Key** field, type the same registration key that you used when you configured the device to be managed by the Defense Center.
- Step 6** From the **Access Control Policy** drop-down list, select an initial policy to apply to the device.

Select the new access control policy created by the configuration import; see [Providing Basic Access Control Settings, page 4-15](#). If you imported multiple configuration packages and therefore the migration process created several access control policies, make sure you select the policy that contains configuration data specific to that device.

**Step 7** If necessary, select the **Protection** check box to apply a model-specific Protection license to the device. So that this migrated deployment can behave equivalently with your Version 4.10.3 deployment, you **must** apply a Protection license to any former Series 3 or virtual 3D Sensor with IPS. You do **not** have to apply Protection licenses to devices in discovery-only deployments, nor do Series 2 devices require a Protection license. For more information, see [Version 5.2 License Requirements, page 3-4](#).

**Step 8** To allow the device to transfer packets to the Defense Center, select the **Transfer Packets** check box in the **Advanced** page area.

This option is enabled by default. If you disable it, you completely prohibit packet transfer to the Defense Center.

**Step 9** Click **Register**.

The device is added to the Defense Center. Note that it may take up to two minutes for the Defense Center to verify the device's heartbeat and establish communication.



**Tip**

The initial access control policy apply may fail, depending on the interface configuration on the device you just added. You can reapply the access control policy later.

**Step 10** After communications are successfully established, continue with [Completing Your Version 5.2 Deployment, page 4-33](#).

## Completing Your Version 5.2 Deployment

After you replace, re-create, reimage, or add devices to the Version 5.2 Defense Center, you should configure all managed devices so they can begin to handle network traffic and report events. In most cases, this is the final step in your migration before placing any out of band devices inline and, optionally, importing legacy events.

For more information, see:

- [Configuring and Verifying Sensing Interfaces and Inline Sets, page 4-33](#)
- [Applying Network Discovery and Access Control Policies, page 4-38](#)

## Configuring and Verifying Sensing Interfaces and Inline Sets

The configuration process for interfaces and inline sets depends on whether you used the sensor migration script or reimaged your sensors manually.

### Completing the Configuration After Reimaging Sensors Using the Sensor Migration Script

When you use the sensor migration script to reimage Version 4.10.3 (or a later patch) sensors, the script also registers your Version 5.2 devices to the Version 5.2.0.x Defense Center and configures your interfaces to match their Version 4.10.3 configurations.

In addition to configuring your interfaces, the sensor migration script also:

- creates a security zone for each Version 4.10.3 passive interface, giving the security zone the same name as the detection engine used by the passive interface
- assigns Version 4.10.3 inline interfaces to a Version 5.2 inline set with **Bypass Mode** enabled for Version 4.10.3 inline with failopen interfaces and disabled for Version 4.10.3 inline only interfaces
- applies your interface configurations to enable detection capability

To complete your sensor migration, Cisco recommends that you view your interface configurations to ensure that they are still appropriate for your Version 5.2 deployment. After verifying your interface configurations, you can continue with the next section, [Applying Network Discovery and Access Control Policies](#), page 4-38.

### Completing the Configuration After Reimaging Sensors Manually

When you reimage devices manually, for your migrated deployment to function properly you must manually configure the interfaces and inline sets on your devices after you add them to the Defense Center.

For your convenience, Cisco provides a script that, when you run it after a configuration import, displays the correct interface configurations for the devices associated with that configuration package.



#### Note

Running the configuration import script cleans up information from any previous invocations. Therefore, if you have multiple unique configuration packages to import, run the display interfaces script **immediately** after each import, and save that script's output to a file that will not be overwritten. Alternately, add and configure all devices referenced in the imported package before you perform the next import.

Run the display interfaces script as the root user from the migration directory (`/var/sf/migration`) using `sudo`, providing your password when prompted. After you log in to the appliance's shell as an Administrator (see [Logging Into an Appliance to Run Migration Scripts](#), page 4-2), the syntax for running the script is as follows:

```
sudo ./display_interfaces.pl
```

Optionally, redirect the output to save it:

```
sudo ./display_interfaces.pl >> my_interface_configs.txt
```

The script provides the name, IP address, and model of each device associated with the most recently imported configuration package, and also provides the following information:

- the link mode and MDI/MDIX settings for the sensing and management interfaces on the device
- for each interface set, the security zone you associated with the set when you imported configurations; see [Creating Security Zones Based on Interface Sets](#), page 4-13
- for each inline interface set, the bypass (failopen) mode and whether tap mode, link state propagation, or transparent inline mode is enabled

As an example:

```
Sensor_A (10.10.123.123) 3D Sensor 8140
=====
eth0 (Management) Mode: 1Gb/Full (Auto) MDI/MDIX: Auto

s1p1 <-> s1p2 Security Zone: failopen interfaces
 Type: failopen Tap mode: off
 Link Propagation: off
 Transparent Inline: on

s1p1 Mode: 1Gb/Full (Auto) MDI/MDIX: Auto
s1p2 Mode: 1Gb/Full (Auto) MDI/MDIX: Auto
```

```

s1p3 <-> s1p4 Security Zone: failopen interfaces
 Type: failopen Tap mode: off
 Link Propagation: off
 Transparent Inline: on

s1p3 Mode: N/A (Auto) MDI/MDIX: Auto
s1p4 Mode: N/A (Auto) MDI/MDIX: Auto

```

Using the output of the display interfaces script as a guide, you can use the Defense Center's web interface to configure the interfaces and inline sets on your managed devices.

You can configure either inline sets or interfaces first depending on your preference. However, keep in mind that if you configure interfaces first, you cannot add them to inline sets until you create the inline sets. On the other hand, if you create inline sets first, you may not be able to add interfaces until you configure the interfaces themselves.

**Note**

After you configure the interfaces and inline sets on a device, you **must** apply the device configuration (**Devices > Device Management**) for your changes to take effect and therefore for your deployment to function properly. After you apply the device configuration, you can continue with [Applying Network Discovery and Access Control Policies](#), page 4-38.

For detailed instructions on configuring interfaces and inline sets, see the *Managing Devices* and *Setting Up an IPS Device* chapters in the *Sourcefire 3D System User Guide*.

**To configure a managed device's interfaces:**

**Access:** Admin/Network Admin

- 
- Step 1** Log into the Defense Center's web interface, then select **Devices > Device Management**.  
The Device Management page appears.
- Step 2** Next to the device whose interfaces you want to configure, click the edit icon (✎).  
The Interfaces tab for that device appears.
- Step 3** Next to the interface you want to edit, click the edit icon (✎).  
The Edit Interface pop-up window appears. The following graphic shows the options for the management interface.

For a sensing device, you can change the type of interface from inline to passive and back. The following graphic shows the options for an inline interface.

The screenshot shows the 'Edit Interface' dialog box with the 'Inline' button selected. The configuration is as follows:

| Field          | Value                               |
|----------------|-------------------------------------|
| Security Zone: | Internal                            |
| Inline Set:    | Default Inline Set                  |
| Enabled:       | <input checked="" type="checkbox"/> |
| Mode:          | Autonegotiation                     |
| MDI/MDIX:      | Auto-MDIX                           |

Buttons: Save, Cancel

372708

The following graphic shows the options for a passive interface.

The screenshot shows the 'Edit Interface' dialog box with the 'Passive' button selected. The configuration is as follows:

| Field          | Value                               |
|----------------|-------------------------------------|
| Security Zone: | None                                |
| Enabled:       | <input checked="" type="checkbox"/> |
| Mode:          | Autonegotiation                     |
| MDI/MDIX:      | Auto-MDIX                           |
| MTU:           | 1518                                |

Buttons: Save, Cancel

372709

**Step 4** Using the output of the display interfaces script as a guide, configure the interface according to the needs of your organization.

If you are able, you can add the interface to an inline set now, or you can do it later when you configure inline sets.

Note that you assign interfaces to security zones individually. You are **not** required to assign all the interfaces in an inline set to the same security zone. Security zones are meant to group multiple interfaces for security purposes; in practice you might, for example, group all ingress interfaces in the same zone regardless of their inline set. For more information on how interfaces, inline sets, and zones interact in Version 5.2, see the *Sourcefire 3D System User Guide*.

**Step 5** Click **Save**.

**To add an inline set:**

**Access:** Admin/Network Admin

**Step 1** Select **Devices > Device Management**.

The Device Management page appears.

**Step 2** Next to the device where you want to add the inline set, click the edit icon (✎).

The Interfaces tab appears.

**Step 3** Click **Inline Sets**.

The Inline Sets tab appears.

**Step 4** Click **Add Inline Set**.

The Add Inline Set pop-up window appears.

**Step 5** Using the output of the display interfaces script as a guide, configure the inline set according to the needs of your organization.

If you are able, you can add inline interface pairs now, or you can do it later when you configure the individual interfaces.



**Tip**

To configure advanced settings for the inline set, such as tap mode, link state propagation, and transparent inline mode, use the **Advanced** tab.

**Step 6** Click **OK**.

## Applying Network Discovery and Access Control Policies

As a final step, to make sure traffic is flowing and being handled correctly, you must apply access control and network discovery policies to the migrated devices in your deployment. First apply access control policies, then the network discovery policy.



**Tip**

After you apply these policies, the migration process is over and you can begin to fine tune your deployment, including recreating any configurations that were not migrated. See [Next Steps, page 4-39](#).

### Applying Access Control Policies

You must apply a **complete** access control policy (which includes intrusion policies) to each migrated device in your deployment.

If performed correctly, the migration process created at least one new access control policy on the Version 5.2 Defense Center, and each of these policies targets one or more of your migrated devices. Apply each of these new policies to its target devices.

#### To quick-apply a complete access control policy:

**Access:** Admin/Security Approver

**Step 1** Log into the Defense Center’s web interface, then select **Policies > Access Control**.

The Access Control page appears.

**Step 2** Click the apply icon (✓) next to the policy you want to apply.

The Apply Access Control Rules pop-up window appears.



**Step 3** Click **Apply All**.

Your policy apply task is queued. Click **OK** to return to the Access Control page.

### Applying the Network Discovery Policy

If you want to perform network and user discovery using your imported configurations, apply the network discovery policy to all the devices in your deployment.

**To apply the network discovery policy:****Access:** Admin/Security Approver

- 
- Step 1** Log into the Defense Center's web interface, then select **Policies > Network Discovery**.  
The Network Discovery Policy page appears.
- Step 2** Click **Apply**.  
A message appears, confirming that you want to apply the policy to all zones targeted by access control policies on the Defense Center.
- Step 3** Click **Yes** to apply the policy.
- 

## Next Steps

After you complete the migration process, Cisco recommends that you complete any administrative tasks you skipped during the initial setup. You may also want to:

- re-create essential configurations that were not migrated; see [Understanding Migrated Configurations and Events, page 5-1](#)
- specify configurations you skipped migrating, for example, local intrusion rules without service metadata
- modify any configurations created by the migration according to the needs of your organization, for example, security zones and inline sets

For detailed information on any the above tasks, the tasks described in the following sections, as well as information on how you can begin to configure your deployment, see the *Sourcefire 3D System User Guide*.

### Individual User Accounts

After you complete the initial setup, the only user on the system is the `admin` user, which has the Administrator role and access. Users with that role have full menu and configuration access to the system, including via the shell or CLI. Cisco recommends that you limit the use of the `admin` account (and the Administrator role) for security and auditing reasons.

Creating a separate account for each person who will use the system allows your organization not only to audit actions and changes made by each user, but also to limit each person's associated user access role or roles. This is especially important on the Defense Center, where you perform most of your configuration and analysis tasks. For example, an analyst needs access to event data to analyze the security of your network, but may not require access to administrative functions for the deployment.

The system includes ten predefined user roles designed for a variety of administrators and analysts. You can also create custom user roles with specialized access privileges.

### Health and System Policies

By default, all appliances have an initial system policy applied. The system policy governs settings that are likely to be similar for multiple appliances in a deployment, such as mail relay host preferences and time synchronization settings. Cisco recommends that you use the Defense Center to apply the same system policy to itself and all the devices it manages.

By default, the Defense Center also has a health policy applied. A health policy, as part of the health monitoring feature, provides the criteria for the system continuously monitoring the performance of the appliances in your deployment. Cisco recommends that you use the Defense Center to apply a health policy to all the devices it manages.

### Software and Database Updates

Cisco recommends that all the appliances in your deployment run the most recent version of the system software. If you plan to use them in your deployment, you should also install the latest intrusion rule updates, vulnerability database (VDB), and geolocation database (GeoDB).



---

**Caution**

Before you update any part of the system software, you **must** read the release notes or advisory text that accompanies the update. The release notes provide important information, including supported platforms, compatibility, prerequisites, warnings, and specific installation and uninstallation instructions.

---



## Understanding Migrated Configurations and Events

---

With very few exceptions, Version 5.2 can perform the same level of intrusion protection, network awareness, and event analysis as Version 4.10.3, and adds many additional features and capabilities. The migration scripts that Cisco provides are designed to allow you to reimage sensors and transfer vital configurations and events from either a Version 4.10.3 Defense Center or a standalone 3D Sensor to a Version 5.2 Defense Center.

In general, you can migrate the following configurations and events:

- intrusion policies, variables, and local rules
- PEP rules from applied PEP policies
- settings from applied RNA detection policies, including networks to monitor
- RNA-related settings in the applied system policy and NetFlow devices specified in the system settings
- compliance policies, compliance rules, and traffic profiles
- 3D Sensor-based RUA configurations
- intrusion and audit events
- interface configurations, when you use the sensor migration script

Note, however, that due to the updated way in which Version 5.2 handles and analyzes traffic, you may not be able to successfully or cleanly migrate specific settings within these configurations.

Any configuration not listed above is **not** migrated, including (but not limited to) unapplied policies; users, preferences, and roles, including LDAP configurations; compliance responses and white lists; RNA detectors and custom fingerprints; health policies; custom workflows, tables, and searches; reports; dashboards; other types of events; and so on. Note that interface configurations are not copied if you do not use the sensor migration script.

This chapter explains which Version 4.10.3 configurations are migrated, including exceptions within those configurations, and how you can expect the migrated settings to appear in Version 5.2.



**Note**

---

This chapter summarizes basic concepts. For detailed information on Version 5.2 features, see the [Version 5.2 Sourcefire 3D System User Guide](#).

---

For more information, see:

- [Understanding the New Access Control Policy, page 5-2](#)

- [Understanding How Interface Sets Become Security Zones](#), page 5-12
- [Understanding How RNA and RUA Settings Are Migrated](#), page 5-13
- [Understanding Migrated Intrusion and Audit Events](#), page 5-18
- [Understanding Migrated Compliance Policies and Rules](#), page 5-18
- [Changes to eStreamer Syntax and Data Structures](#), page 5-19

## Understanding the New Access Control Policy

*Access control* is a new policy-based feature that allows you to specify, inspect, and log the traffic that can traverse your network. An *access control policy*, which you apply to one or more *target devices*, determines how the system handles traffic on your network.

Along with many added features for Version 5.2, access control policies can perform the following analysis and traffic handling that you could also perform in Version 4.10.3:

- Using access control rules with access control policies, you can duplicate the functionality of most PEP rules to trust (sometimes called *fast path*) specific traffic.
- Using access control rules, you can invoke intrusion policies to analyze, and optionally block, traffic based on intrusions and exploits.
- Access control policies define the traffic that you permit and, therefore, the traffic you can monitor with the discovery feature (previously called *RNA*).

The migration process creates a new access control policy on the Version 5.2 Defense Center every time you import a configuration package from either a Version 4.10.3 3D Sensor or Defense Center.

Note that if the import script cannot build an access control policy using the configurations in an exported Version 4.10.3 package (for example, because the package does not contain the necessary configurations), the script creates a new access control policy with no rules and using Version 5.2 defaults.

After you finish the import process and modify the new access control policy to accommodate any configurations not migrated, you can apply the policy; see [Applying Network Discovery and Access Control Policies](#), page 4-38.

### Target Devices

An access control policy target device, or *target*, is simply a device where you apply the policy. When you add devices to the Version 5.2 Defense Center after you complete the configuration import, you specify the access control policies to apply to those devices. The Defense Center adds the devices as targets for the appropriate policies.

### Access Control Rules

*Access control rules* in an access control policy define how traffic is handled by managed devices. These rules can allow, monitor, inspect, or block traffic based on multiple criteria. They can perform simple IP matching, or create complex scenarios involving different networks, users, applications, ports, and URLs.

The migration process adds rules to the new access control policy based on your Version 4.10.3 PEP rules, applied intrusion policies, and RNA detection policy settings.

### Default Action

When you import configurations onto the Defense Center, you name the new access control policy and specify its default action; see [Providing Basic Access Control Settings, page 4-15](#). In Version 5.2, the access control policy's *default action* specifies how the system handles traffic that does not meet the conditions of any access control rule in an access control policy.

The script prompts you to select an intrusion policy to associate with the default action, and using it to inspect all default-action traffic. You can choose any intrusion policy that exists on the Version 5.2 Defense Center, or you can choose one from the configuration package you are importing. The script lists both system-provided and user-created policies. The default is to associate the system-provided Balanced Security and Connectivity intrusion policy with the default action.

You can also create a default action that is **not** associated with an intrusion policy, but that allows all default-action traffic to be inspected by network discovery. This is useful in discovery-only (RNA-only) deployments.

### Logging

Connection logging (formerly flow data logging) is now configured as part of access control, rather than as a part of network discovery. The migration process uses the flow data collection preferences in your Version 4.10.3 RNA detection policies to set connection logging preferences for each access control rule and the access control policy default action. However, this split complicates the migration of Version 4.10.3 port exclusion preferences. The migration must create multiple access control rules for combinations of intrusion inspection and port exclusions so that you do not log specified traffic.

See the following sections for more information:

- [Migrating PEP Rules into Access Control Rules, page 5-3](#)
- [Migrating Intrusion Policies and Creating Access Control Rules, page 5-4](#)
- [Migrating RNA Settings into Rules and Logging Preferences, page 5-7](#)
- [Example Migrated Access Control Rules, page 5-10](#)

## Migrating PEP Rules into Access Control Rules

PEP was a feature in Version 4.10.3 that allowed you to create rules to block or send traffic directly through some 3D Sensors with no further inspection.



### Note

Of the two components of PEP policies in Version 4.10.3 (fast-path rules and PEP rules), only IPv4 and IPv6 PEP rules in applied PEP policies are migrated into access control rules. Version 4.10.3 fast-path rules are **not** migrated; you must configure these rules at the device level after you add devices to your Version 5.2 deployment. For more information, see the *Managing Devices* chapter in the [Version 5.2 Sourcefire 3D System User Guide](#).

The migration places PEP-created access control rules at the top of the new access control policy so that they are evaluated first. The migration also prioritizes IPv6 PEP rules over IPv4 PEP rules. Note that only PEP rules in applied, non-deleted policies can be migrated.

The migration converts PEP rules to access control rules as described in the following table.

Table 5-1 PEP Rule Migration

| If the PEP Rule action was...                                                                                               | The access control rule action is... | And the PEP rule becomes...                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Drop                                                                                                                        | Block                                | a single access control rule that blocks the traffic specified by the PEP rule. Blocked traffic is not subject to inspection of any kind.                                                                                                                                                                                                             |
| Drop w/ Reset                                                                                                               | Block with reset                     | a single access control rule that blocks the traffic specified by the PEP rule, and resets the connection. Blocked traffic is not subject to inspection of any kind.                                                                                                                                                                                  |
| Fast Path (or DE Specific where IPS, RNA, and RUA are all set to Fast Path)                                                 | Trust                                | a single access control rule that trusts the traffic specified by the PEP rule. Trusted traffic is not subject to inspection of any kind.                                                                                                                                                                                                             |
| Analyze (or DE Specific where IPS, RNA, and RUA are all set to Analyze)                                                     | Allow                                | a set of access control rules that ensures all traffic specified by the PEP rule is inspected.<br><br>The network conditions for these access control rules represent the intersection of the networks in the PEP rule and all other rules in the new access control policy.                                                                          |
| DE Specific: <ul style="list-style-type: none"> <li>• IPS set to Fast Path</li> <li>• RNA and RUA set to Analyze</li> </ul> | Allow                                | a set of access control rules that ensures all traffic specified by the PEP rule is eligible to be monitored by discovery, but is not inspected by an intrusion policy.<br><br>The network conditions for these access control rules represent the intersection of the networks in the PEP rule and all other rules in the new access control policy. |
| DE Specific: <ul style="list-style-type: none"> <li>• IPS set to Analyze</li> <li>• RNA or RUA set to Fast Path</li> </ul>  | n/a                                  | Because of the way Version 5.2 access control rules handle traffic, you cannot have traffic bypass discovery (RNA or RUA) but still be analyzed by an intrusion policy (IPS).<br><br>These PEP rules <b>cannot</b> be migrated; see <a href="#">Resolving Unsupported RNA and RUA Fast-Path PEP Rules</a> , page 4-12.                                |

## Migrating Intrusion Policies and Creating Access Control Rules

The migration transfers all applied Version 4.10.3 intrusion policies and settings into Version 5.2 intrusion policies as-is, with the following exceptions:

- VLAN and network filtering (that is, using an intrusion policy to monitor a specific VLAN or subnetwork) has moved out of the intrusion policy and into the access control rule that invokes the policy.
- Intrusion policies can no longer target detection engines. In Version 5.2, access control rules determine which intrusion policies examine which traffic.
- With Version 5.2, you can no longer explicitly configure IPS detection engine variables.
- You must add service metadata (a new requirement) to all local intrusion rules that inspect traffic on specific ports.
- OPSEC configurations within a Version 4.10.3 intrusion policy are not migrated because Version 5.2 does not support OPSEC configuration.

Note that although it is no longer in the intrusion policy, the migration process converts VLAN and target information into equivalent settings in the access control policy. The migration process can also migrate detection variables at the cost of a proliferation of intrusion policies.

Version 5.2 intrusion policies are named the same as their Version 4.10.3 counterparts. Intrusion policies created to handle custom detection engine variables reference the detection engine, for example:

```
policy_name (copy for variables from 'detection_engine')
```

For more information, see:

- [Understanding Access Control Rules That Perform Intrusion Inspection, page 5-5](#)
- [Migrating Detection Engine Variables Into Policy Variables, page 5-7](#)
- [Adding Service Metadata to Intrusion Rules, page 4-11](#)

## Understanding Access Control Rules That Perform Intrusion Inspection

In Version 5.2, access control rules determine which intrusion policies examine which traffic. To migrate this functionality, each Version 4.10.3 intrusion policy-detection engine pair in Version 4.10.3 creates at least one access control rule.

- An **unfiltered** (not restricted by network or VLAN) intrusion policy applied to one detection engine creates **one** access control rule that invokes that intrusion policy.
- A VLAN-or-network **filtered** policy creates **two** rules that invoke that intrusion policy: one rule has a network condition that matches source traffic, the other, destination traffic.

Each access control rule is also restricted by security zone (collection of interfaces), which ensures that the rule's associated intrusion policy monitors only the traffic flowing through certain interfaces.

The following table explains how specific access control rule settings depend on your Version 4.10.3 configurations. All other settings in the created access control rules use Version 5.2 defaults. Note that only filtered policies have network and VLAN conditions.

**Table 5-2** Migrated Access Control Rule Settings

| Version 4.10.3 Policy Type | Access Control Rule Setting                                                                                             | Details                                                                                                                                                                                                                                                                                                                                    |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all                        | <b>Action</b> , which determines how matching traffic is handled and inspected                                          | All access control rules created to perform intrusion inspection must have an action of Allow.                                                                                                                                                                                                                                             |
| all                        | <b>Enabled</b> , which determines whether the rule is used                                                              | Access control rules created by the migration are enabled by default.                                                                                                                                                                                                                                                                      |
| all                        | <b>Source Zones</b> (Zone tab), which determines the interfaces whose traffic the rule examines                         | Restricting access control rules by zone preserves the Version 4.10.3 setting where each intrusion policy was applied to an IPS detection engine, which would monitor the traffic flowing through a specified interface set. For more information, see <a href="#">Understanding How Interface Sets Become Security Zones, page 5-12</a> . |
| all                        | <b>Intrusion Policy</b> (Inspection table)                                                                              | All access control rules created to perform intrusion inspection have an associated intrusion policy.                                                                                                                                                                                                                                      |
| all                        | enabled <b>Log at End of Connection</b> and <b>Send Connection Events to Defense Center</b> settings on the Logging tab | The logging settings for an access control rule depend on settings in your Version 4.10.3 RNA detection policies. For more information, see <a href="#">Migrating RNA Settings into Rules and Logging Preferences, page 5-7</a> .                                                                                                          |

Table 5-2 Migrated Access Control Rule Settings (continued)

| Version 4.10.3 Policy Type | Access Control Rule Setting                                   | Details                                                                                                                                                                                                                                                                            |
|----------------------------|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| network-filtered           | <b>Source Networks or Destination Networks</b> (Networks tab) | Access control rules created to inspect traffic with a network-filtered intrusion policy use the deprecated <b>Policy by VLAN or Network</b> settings from the Version 4.10.3 intrusion policy to specify source and destination network constraints for the access control rules. |
| VLAN-filtered              | <b>Selected VLAN Tags</b> (VLAN Tags tab)                     | Access control rules created to inspect traffic with a VLAN-filtered intrusion policy use the deprecated <b>Policy by VLAN or Network</b> settings from the Version 4.10.3 intrusion policy to specify VLAN constraints for the access control rules.                              |

Access control rules based on intrusion policies use the following naming syntax:

```
policy <non-filtered|<src IP|dst IP|vlan tag#>> on zone
```

where:

- *policy* is the name of the applied policy, or policy copy in the case of custom detection engine variables.
- *IP* is the source or destination network configuration derived from the **Network** field in a Version 4.10.3 network-filtered policy.
- *tag#* is the VLAN tag configuration derived from the **VLAN** field in a Version 4.10.3 VLAN-filtered policy.
- *zone* is the security zone created from the interface set configured on the detection engine where the migrated policy was applied.

Access control rules created by the migration process have long, descriptive names for your convenience. If you edit these rules, you must rename them using no more than 30 characters before you save them. The following table provides example names for different access control rules derived from an intrusion policy named *MyPolicy*.

Table 5-3 Example Access Control Rules Names

| Policy Configuration                                                                                        | Access Control Rule Name                                                                                    |
|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| non-filtered policy                                                                                         | MyPolicy non-filtered on Myzone                                                                             |
| non-filtered policy applied to three detection engines                                                      | MyPolicy non-filtered on Myzone-1<br>MyPolicy non-filtered on Myzone-2<br>MyPolicy non-filtered on Myzone-3 |
| VLAN-filtered policy with VLAN tags 1, 2, and 3 configured                                                  | MyPolicy vlan 1,2,3 on Myzone                                                                               |
| network-filtered policy (source rule) with IP addresses 10.1.1.1, 10.1.1.2, and 10.5.0.0/16 configured      | MyPolicy src 10.1.1.1, 10.1.1.2, 10.5.0.0/16 on Myzone                                                      |
| network-filtered (policy destination rule) with IP addresses 10.1.1.1, 10.1.1.2, and 10.5.0.0/16 configured | MyPolicy dst 10.1.1.1, 10.1.1.2, 10.5.0.0/16 on Myzone                                                      |
| non-filtered policy applied to detection engine DE-x with custom variables                                  | MyPolicy (copy for variables on 'DE-x') non-filtered on Myzone                                              |

**Table 5-3 Example Access Control Rules Names (continued)**

| Policy Configuration                                                                                                   | Access Control Rule Name                                       |
|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| VLAN-filtered policy with VLAN tag 1, applied to detection engine DE-x with custom variables                           | MyPolicy (copy for variables on 'DE-x') vlan 1 on Myzone       |
| network-filtered policy (source rule) with IP address 10.5.1.2, applied to detection engine DE-x with custom variables | MyPolicy (copy for variables on 'DE-x') src 10.5.1.2 on Myzone |

## Migrating Detection Engine Variables Into Policy Variables

In the Sourcefire 3D System, a variable is a representation of a port or network value that is commonly used in intrusion rules. Rather than hard-coding these values in multiple rules, you can tailor a rule to accurately reflect your network environment by changing the variable value.

In Version 4.10.3 you could configure custom variables for IPS detection engines, which had priority over intrusion policy-specific variables which, in turn, had priority over system variables. The migration transfers your policy-specific variables to Version 5.2, and also creates a system variable for each migrated policy-specific variable, using the same variable name and a value of `any`.

However, with Version 5.2, you no longer explicitly configure detection engines or detection engine variables. This means that you cannot cleanly migrate a Version 4.10.3 intrusion policy applied to IPS detection engines that use custom variables.

To replicate Version 4.10.3 functionality and migrate custom detection engine variables, the import script can create a copy of the intrusion policy for each active detection engine that used custom variables. These copies use the original intrusion policy as the base policy; each one has different policy-specific variables that correspond to one of the Version 4.10.3 custom variable sets.

Because this can result in a proliferation of intrusion policies, the import script prompts you whether to create the copies. If you decline, the script does not migrate custom detection engine variables and your Version 5.2 configurations will use only the parent intrusion policy.

For Version 4.10.3 IPS detection engines with custom variables but without an intrusion policy applied, the migration converts each custom variable to a system variable using the same variable name and a value of `any`.

## Migrating RNA Settings into Rules and Logging Preferences

In Version 4.10.3, you configured host discovery and flow data logging in RNA detection policies. In Version 5.2, logging and monitoring functionality is split: the access control policy governs which connections (flows) are logged on a per-access control rule basis, but the network discovery policy governs discovery.

The migration process uses the flow data logging settings in your applied Version 4.10.3 RNA detection policies to determine how to configure connection logging in the Version 5.2 access control policy, which is done using access control rules.

- To exclude traffic to and from a specific port (on one or more hosts) from connection logging while preserving logging and inspection for other hosts, the migration must create **multiple** access control rules for combinations of intrusion inspection and port exclusion preferences.

- To log (or exclude from logging) connections for a particular network, the migration adds **two** access control rules for each network to monitor-detection engine combination in the Version 4.10.3 RNA detection policy, once for source traffic and one for destination traffic. For example, if an RNA detection policy is applied to three different detection engines, the migration adds six access control rules.

#### Access Control Rule Order

The system places port exclusion-based rules above rules based on networks to monitor or exclude. For example, note the Version 4.10.3 network configurations in the following graphic:

- network to monitor: 10.0.0.0/8
- excluded network: 10.1.0.0/16
- excluded ports: 80 (tcp) on 10.2.0.0/16 in source/destination traffic

#### ▼ Networks to Monitor



| IP Address | Netmask | Data Collection    | Reporting Detection Engine |        |
|------------|---------|--------------------|----------------------------|--------|
| 10.0.0.0   | 8       | Host and Flow Data | RNA1-DE                    | Delete |
| ! 10.1.0.0 | 16      | Exclude            | RNA1-DE                    | Delete |

#### ▼ Ports to Exclude



| Port(s) | Protocol | Source/Destination | IP Address | Netmask |        |
|---------|----------|--------------------|------------|---------|--------|
| 80      | tcp      | Source/Destination | 10.2.0.0   | 16      | Delete |

372705

The following graphic shows the access control rules for the migrated configurations in the example. Note that, for clarity, not all columns are shown.

| #                              | Name                                                             | Source Networks                                       | Dest Networks   | Src Ports  | Dest Ports | Action  |                                                                                                                                                                                                                                                             |
|--------------------------------|------------------------------------------------------------------|-------------------------------------------------------|-----------------|------------|------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Administrator Rules</b>     |                                                                  |                                                       |                 |            |            |         |                                                                                                                                                                                                                                                             |
| <i>This category is empty.</i> |                                                                  |                                                       |                 |            |            |         |                                                                                                                                                                                                                                                             |
| <b>Standard Rules</b>          |                                                                  |                                                       |                 |            |            |         |                                                                                                                                                                                                                                                             |
| 1                              | Exclude logs on zone 1 for dst 10.2.0.0/16 dest ports TCP (6):80 | any                                                   | 10.2.0.0/16 any | TCP (6):80 |            | Allow   |    |
| 2                              | Exclude logs on zone 1 for src 10.2.0.0/16 src ports TCP (6):80  | 10.2.0.0/16                                           | any             | TCP (6):80 | any        | Allow   |    |
| 3                              | Exclude logs on zone 1 for dst 10.1.0.0/16                       | any                                                   | 10.1.0.0/16     | any        | any        | Allow   |    |
| 4                              | Exclude logs on zone 1 for src 10.1.0.0/16                       | 10.1.0.0/16                                           | any             | any        | any        | Allow   |    |
| 5                              | flow logging for dst 10.0.0.0/8 on 1                             | any                                                   | 10.0.0.0/8      | any        | any        | Monitor |    |
| 6                              | flow logging for src 10.0.0.0/8 on 1                             | 10.0.0.0/8                                            | any             | any        | any        | Monitor |    |
| <b>Root Rules</b>              |                                                                  |                                                       |                 |            |            |         |                                                                                                                                                                                                                                                             |
| <i>This category is empty.</i> |                                                                  |                                                       |                 |            |            |         |                                                                                                                                                                                                                                                             |
| <b>Default Action</b>          |                                                                  | Intrun Prevention: Balanced Security and Connectivity |                 |            |            |         |                                                                                                                                                                                                                                                             |

Note the following configurations in the second graphic:

- Rules 1 and 2 allow traffic for the excluded port 80 on 10.2.0.0/16 to proceed without further processing.
- Rules 3 and 4 allow traffic for the excluded network 10.1.0.0/16 to proceed without further processing.
- Rules 5 and 6 monitor remaining traffic on network 10.0.0.0/8. The logging icon () for these rules indicates that the system logs connections in matching traffic.

The following table describes the configuration of each access control rule created from an applied intrusion policy.

**Table 5-4 Migrated Access Control Rule Settings**

| Version 4.10.3 Configuration         | Version 5.2 Access Control Rule Setting                                                                   | Details                                                                                                                                                                                                                                                          |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a network to monitor                 | an <b>Action of Monitor</b><br><b>Source Networks</b> or<br><b>Destination Networks</b><br>(Networks tab) | Access control rules created to log connections have an action of <b>Monitor</b> to ensure that logging is enabled. This action also allows traffic to match subsequent access control rules.<br><br>These rules also specify which network they are monitoring. |
| a network to exclude from monitoring | an <b>Action of Allow</b>                                                                                 | Access control roles created to allow traffic to pass without logging have an action of <b>Allow</b> but disabled logging options. These rules have an associated intrusion policy if your Version 4.10.3 deployment monitored that network with one.            |

Table 5-4 Migrated Access Control Rule Settings (continued)

| Version 4.10.3 Configuration                              | Version 5.2 Access Control Rule Setting                                                                                 | Details                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a port to exclude from monitoring                         | an <b>Action of Allow</b><br><b>Selected Destination Ports</b><br>or <b>Selected Source Ports</b><br>(Ports tab)        | Access control roles created to allow port-based traffic to pass without logging or inspection have an action of <b>Allow</b> , but no associated intrusion policy or logging options.<br>These rules also specify which ports and protocols they are excluding.                                                                                      |
| <b>Reporting Detection Engine</b> for a network           | <b>Zones</b> (Zones tab)                                                                                                | Restricting logging by zone preserves the Version 4.10.3 setting where each network was monitored by a specific RNA detection engine, which would log the traffic flowing through a specified interface set. For more information, see <a href="#">Understanding How Interface Sets Become Security Zones</a> , page 5-12.                            |
| <b>Host and Flow Data</b> collection option for a network | enabled <b>Log at End of Connection</b> and <b>Send Connection Events to Defense Center</b> settings on the Logging tab | The logging settings for an access control rule depends on settings in your Version 4.10.3 RNA detection policies. For more information, see <a href="#">Migrating RNA Settings into Rules and Logging Preferences</a> , page 5-7.                                                                                                                    |
| n/a                                                       | <b>Intrusion Policy</b><br>(Inspection table)                                                                           | All access control rules created to perform intrusion inspection have an associated intrusion policy. Whether an access control rule that logs connections has an associated intrusion policy depends on your Version 4.10.3 intrusion configurations; see <a href="#">Migrating Intrusion Policies and Creating Access Control Rules</a> , page 5-4. |
| n/a                                                       | <b>Enabled</b> , which determines whether the rule is used                                                              | Access control rules created by the migration are enabled by default.                                                                                                                                                                                                                                                                                 |

## Example Migrated Access Control Rules

The following graphic includes example access control rules for each type of configuration that populates the access control policy created by the migration.

| Standard Rules |                                                                                                                               |
|----------------|-------------------------------------------------------------------------------------------------------------------------------|
| 1              | ⚠ PEP analyze (src 10.3.1.0/24 dst 10.3.2.0/24) + (Example Applied Network Filtered Policy dst dst 10.0.0.0/8 on interface 1) |
| 2              | ⚠ PEP analyze (src 10.3.1.0/24 dst 10.3.2.0/24) + (Example2 Applied Unfiltered Policy non-filtered on interface 1)            |
| 3              | ⚠ PEP fastpath src 10.5.1.0/24 dst 10.5.2.0/24                                                                                |
| 4              | ⚠ PEP drop src 10.2.1.0/24 dst 10.2.2.0/24                                                                                    |
| 5              | ⚠ Example Applied Network Filtered Policy dst 10.0.0.0/8 on interface 1                                                       |
| 6              | ⚠ Example Applied Network Filtered Policy src 10.0.0.0/8 on interface 1                                                       |
| 7              | ⚠ Example2 Applied Unfiltered Policy non-filtered on interface 1                                                              |
| 8              | ⚠ flow logging for dst 10.4.0.0/16 on interface 3                                                                             |
| 9              | ⚠ flow logging for src 10.4.0.0/16 on interface 3                                                                             |
| 10             | ⚠ Example Applied VLAN Filtered Policy vlan 1 on interface 3                                                                  |
| 11             | ⚠ Example Applied Unfiltered Policy non-filtered on interface 3                                                               |
| 12             | ⚠ Example Applied Intrusion Policy non-filtered on interface 2 - exclude logs for src 10.5.2.0/24 src ports TCP (6):80        |
| 13             | ⚠ Example Applied Intrusion Policy non-filtered on interface 2 - exclude logs for dst 10.5.2.0/24 dest ports TCP (6):80       |
| 14             | ⚠ Example Applied Intrusion Policy non-filtered on interface 2 - exclude logs for dst 10.5.1.0/24                             |
| 15             | ⚠ Example Applied Intrusion Policy non-filtered on interface 2 - exclude logs for src 10.5.1.0/24                             |
| 16             | ⚠ flow logging for dst 10.5.0.0/16 on interface 2                                                                             |
| 17             | ⚠ flow logging for src 10.5.0.0/16 on interface 2                                                                             |
| 18             | ⚠ Example Applied Intrusion Policy non-filtered on interface 2                                                                |

372702

The warning (⚠) icons in the graphic indicate that interfaces for the rules are not yet configured. The following table describes the rules in the graphic.

**Table 5-5** Example Access Control Rules

| This Rule... | Appears Because the Exported Configurations Included...                                                                                                                                                                                                                                                                                                               |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1, 2         | a PEP rule with the action Analyze, an initiator in the network 10.3.1.0/24, and a responder in the network 10.3.2.0/24; the rule intersects with network 10.0.0.0/8 targeted in the network-filtered policy <i>Example Applied Network Filtered Policy</i> . The complexities of the migration, including the presence of rules 3 and 4, make these rules necessary. |
| 3            | a PEP rule with the action Fast Path, an initiator in the network 10.5.1.0/24, and a responder in the network 10.5.2.0/24.                                                                                                                                                                                                                                            |

Table 5-5 Example Access Control Rules (continued)

| This Rule... | Appears Because the Exported Configurations Included...                                                                                                                                                                                                                                                |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4            | a PEP rule with the action Drop, an initiator in the network 10.2.1.0/24, and a responder in the network 10.2.2.0/24.                                                                                                                                                                                  |
| 5, 6         | a network-filtered intrusion policy targeting the network 10.0.0.0/8 and named <i>Example Applied Network Filtered Policy</i> ; the policy was applied to a detection engine that used an interface that was migrated to a zone named <i>interface 1</i> .                                             |
| 7            | an unfiltered intrusion policy named <i>Example2 Applied Unfiltered Intrusion Policy</i> which; the policy was applied to a detection engine that used an interface that was migrated to a zone named <i>interface 1</i> .                                                                             |
| 8, 9         | an RNA detection policy configured to monitor hosts and flow data on the 10.4.0.0/16 network; the policy was applied to a detection engine that used an interface that was migrated to a zone named <i>interface 3</i> . Note that this detection policy did not include networks or ports to exclude. |
| 10           | a VLAN-filtered intrusion policy targeting VLAN 1 and named <i>Example Applied VLAN Filtered Policy</i> ; the policy was applied to a detection engine that used an interface that was migrated to a zone named <i>interface 3</i> .                                                                   |
| 11           | an unfiltered intrusion policy named <i>Example Applied Unfiltered Policy</i> ; the policy was applied to a detection engine that used an interface that was migrated to a zone named <i>interface 3</i> .                                                                                             |
| 13, 12       | an exclusion in the RNA detection policy monitoring network 10.5.0.0/16 to prevent logging connections for TCP port 80 in the network 10.5.2.0/24.                                                                                                                                                     |
| 15, 14       | an exclusion in the RNA detection policy monitoring network 10.5.0.0/16 to prevent logging connections in the network 10.5.1.0/24.                                                                                                                                                                     |
| 17, 16       | an RNA detection policy configured to monitor hosts and flow data on the 10.5.0.0/16 network; the policy was applied to a detection engine that used an interface that was migrated to a zone named <i>interface 2</i> .                                                                               |
| 18           | an unfiltered intrusion policy named <i>Example Applied Intrusion Policy</i> ; the policy was applied to a detection engine that used an interface that was migrated to a zone named <i>interface 2</i> .                                                                                              |

## Understanding How Interface Sets Become Security Zones

The Version 4.10.3 concept of interface sets is replaced by the Version 5.2 concept of *security zones*, which are groupings of one or more interfaces that you can use to manage and classify traffic flow in various policies and configurations. The interfaces in a single zone may span multiple devices; you can also configure multiple zones on a single device. Using zones allows you to divide the network into segments where you can apply various policies. You must assign at least one interface to a security zone to match traffic against that security zone, and each interface can belong to only one zone. Note that the sensor migration script automatically assigns migrated passive interfaces (but not inline or inline with failopen interfaces) to security zones. See [Completing Your Version 5.2 Deployment, page 4-33](#).



### Tip

In Version 5.2, an *inline set* refers to one or more pairs of inline interfaces that you group to streamline the applying of various networking settings. Inline sets are unrelated to security zones; not all the ingress interfaces in an inline set must belong to the same zone.

In addition to using security zones to group interfaces, you can use zones in various places in the system's web interface, including access control policies, network discovery rules, and event searches. For example, you could write an access control rule that applies only to a specific source or destination zone, or restrict network discovery to traffic to or from a specific zone.

For each active Version 4.10.3 detection engine in the package you are importing, the configuration import script prompts you to create a security zone on the Defense Center; see [Creating Security Zones Based on Interface Sets](#), page 4-13. Each zone is meant to contain the interfaces in the Version 4.10.3 interface sets monitored by each detection engine.

**Note**

Although the configuration import script can create security zones, if you want to match traffic against those zones you must **manually** assign the interfaces on migrated Version 5.2 devices to those zones **after** you add your migrated Version 5.2 devices to the Defense Center. Note that the sensor migration script automatically assigns passive (but not inline or inline with failopen) interfaces to zones. For more information, see [Configuring and Verifying Sensing Interfaces and Inline Sets](#), page 4-33.

When the import script runs, it uses the zones you create to configure rules within the new access control policy and the migrated network discovery rules.

For example, consider a 3D Sensor:

- with an IPS detection engine named `IPS_DE`
- monitoring a inline interface set named `inline_interfaces`
- using an unfiltered intrusion policy named `no_exploits`

If you accept the defaults, the import script:

- creates a Version 5.2 security zone named `inline_interfaces` where you should assign the interfaces that were in the Version 4.10.3 `inline_interfaces` set, and
- creates an access control rule that uses the `no_exploits` intrusion policy to inspect traffic flowing over interfaces in the `inline_interfaces` zone

**Tip**

When configuring a migrated device's interfaces and inline sets, you are **not** required to assign all the interfaces in an inline set to zones created by the import script, although you may want to for the initial configuration and policy apply steps. Zones are meant to group multiple interfaces for security purposes; in practice you might, for example, group all ingress interfaces in the same zone regardless of their inline set. For more information on how interfaces, inline sets, and zones interact in Version 5.2, see the [Version 5.2 Sourcefire 3D System User Guide](#).

## Understanding How RNA and RUA Settings Are Migrated

In Version 4.10.3, the most critical piece of your RNA deployment is the RNA detection policy. When applied to RNA detection engines on managed 3D Sensors with RNA, the detection policy controls how RNA events and flow data are collected:

- General settings govern policy-specific data collection preferences.
- A list of networks that you specify tells the system which traffic to monitor and log; you can also specify networks that you are monitoring with NetFlow-enabled devices.
- You can specify a list of ports (for specific IP addresses) that you want to exclude from monitoring and logging.

Also in Version 4.10.3, you could collect user activity using 3D Sensors with RUA by creating an RUA detection engine and assigning it to monitor traffic flowing through a specific interface set.

Various settings in the Version 4.10.3 system policy and system settings govern RNA data storage, impact flag correlation, operating system and service identity conflicts, RUA protocol monitoring, NetFlow settings, and so on.

With very few exceptions, Version 5.2 can monitor and log traffic identically to Version 4.10.3, and also adds some capabilities. However, the way you configure discovery (RNA), user awareness (RUA), and connection logging (flow data logging) is now different, and some settings have moved:

- RNA detection policies have been replaced by a single network discovery policy, which you apply to all devices managed by a Defense Center. Using discovery rules, the network discovery policy specifies which security zones, networks, and ports your devices monitor to generate host, application and user data. The network discovery policy includes NetFlow configurations.
- Because you no longer need to configure common settings across multiple detection policies, settings that were in the Version 4.10.3 system policy are now in the network discovery policy.
- You now configure user detection by 3D Sensors wholly within the network discovery policy; any traffic that you can inspect for host data you can inspect for user data. You no longer configure RUA detection engines or restrict detection protocols in the system settings.
- Connection logging (with the exception of NetFlow logging) has moved to the access control policy, where you configure it on a per-access control rule basis. For more information, see [Migrating RNA Settings into Rules and Logging Preferences, page 5-7](#).

Where possible, the configuration import script gracefully migrates your Version 4.10.3 settings to their Version 5.2 counterparts. Your Version 4.10.3 Networks to Monitor settings in your applied RNA detection policies become discovery rules, your old system policy settings are preserved in the network discovery policy, and so on.

Note that in most cases, you will only have one applied detection policy per Defense Center. If you have two applied detection policies, their rules represent a merged version of the networks to monitor, as long as there are no detection engine conflicts in your Version 4.10.3 configurations; see [Assigning One Detection Engine of Each Type to Interface Sets, page 4-10](#). Similarly, if you have existing discovery rules in your Version 5.2 network discovery policy, the migration merges them with the rules it creates.


**Note**


---

Only user activity detection by 3D Sensors is migrated. User Agent settings and associated LDAP authorization objects are **not** migrated; you must recreate those configurations after the migration.

---

For more information on how RNA and RUA configurations are migrated, see:

- [Understanding How The Migration Creates Discovery Rules, page 5-14](#)
- [Migrating Other RNA and RUA Settings, page 5-16](#)

## Understanding How The Migration Creates Discovery Rules

The migration process converts the Version 4.10.3 Networks to Monitor and Ports to Exclude settings in your applied RNA detection policies into Version 5.2 discovery rules in the single network discovery policy:

- Each **network** you monitor or exclude creates **one** discovery rule that monitors that network.

These rules can then be converted to **multiple** discovery rules, depending on your **port exclusions**. The number of rules and the networks monitored by each of the rules depends on the *intersection* of your port-excluded hosts with the networks you were monitoring in Version 4.10.3.

- Each **NetFlow network** you monitor or exclude creates **one** discovery rule that monitors that network.

Discovery rules govern whether and how the system collects information on your network's hosts including the operating systems, active applications, and user activity on those hosts.

**Note**

Version 5.2 discovery rules do **not** govern connection logging for your network traffic; that capability has moved to access control. For more information, see [Migrating RNA Settings into Rules and Logging Preferences, page 5-7](#).

Each discovery rule is also restricted by security zone, which ensures that the system uses the rule to examine only the traffic flowing through certain interfaces. (A zone is a collection of interfaces.)

The following table explains how specific discovery rule settings depend on your Version 4.10.3 configurations. All other settings in the created discovery rules use Version 5.2 defaults. Remember that these settings apply to monitoring **only** and not logging.

**Table 5-6 RNA Settings Migrated to Discovery Rules**

| Version 4.10.3 Policy Configuration                                                    | Version 5.2 Discovery Rule Setting                                                      | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Address and Netmask in the Networks to Monitor section                              | <b>Networks</b> (Network tab)                                                           | Depending on how your Version 4.10.3 networks to monitor intersected with your port exclusions, each discovery rule created by the migration monitors <b>all or part</b> of a single network to monitor in Version 5.2.                                                                                                                                                                                                                                                                                                                                   |
| settings in the Ports to Exclude section, including <b>Port(s)</b> and <b>Protocol</b> | <b>Selected Destination Ports</b> or <b>Selected Source Ports</b> (Port Exclusions tab) | Discovery rules created by the migration exclude source or destination ports from monitoring for the rule's specified network depending on your settings in the Version 4.10.3 RNA detection policy.                                                                                                                                                                                                                                                                                                                                                      |
| <b>Exclude</b> data collection option for a network                                    | an <b>Action of Exclude</b>                                                             | If you excluded a network (including a NetFlow network) from monitoring in Version 4.10.3, that network is also excluded in Version 5.2 using a discovery rule with an <b>Action of Exclude</b> .                                                                                                                                                                                                                                                                                                                                                         |
| <b>Host Data Only</b> or <b>Host and Flow Data</b> collection option for a network     | an <b>Action of Discover</b>                                                            | If you monitored a network for host data in Version 4.10.3, that network is also monitored in Version 5.2 using a discovery rule with an <b>Action of Discover</b> . This also applies to NetFlow networks to monitor.<br><br>This new rule enables both <b>Hosts</b> and <b>Applications</b> discovery on those networks, to help you build the network map. It also enables <b>Users</b> discovery when, in Version 4.10.3, you used an RUA detection engine to monitor the traffic now represented by the discovery rule's security zone restrictions. |

**Table 5-6** RNA Settings Migrated to Discovery Rules (continued)

| Version 4.10.3 Policy Configuration                                                                         | Version 5.2 Discovery Rule Setting                                             | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| the <b>Generate Hosts from NetFlow Data</b> and <b>Generate Services from NetFlow Data</b> general settings | an <b>Action of Log NetFlow Connections</b> if both these options are disabled | If you had these settings disabled in Version 4.10.3, when the migration creates discovery rules based on your NetFlow networks to monitor, an <b>Action of Log NetFlow Connections</b> ensures that NetFlow-discovered hosts and applications are <b>not</b> added to the network map, but NetFlow connections are still logged.                                                                                                                                                                            |
| <b>Reporting Detection Engine</b> for each network to monitor                                               | <b>Zones</b> (Zones tab)                                                       | Restricting discovery by zone preserves the Version 4.10.3 setting where each network was monitored by a specific RNA detection engine, which would monitor the traffic flowing through a specified interface set. For more information, see <a href="#">Understanding How Interface Sets Become Security Zones, page 5-12</a> .<br><br><b>Note</b> Subnet detection is <b>not</b> supported in Version 5.2 because of the deprecation of detection engines and the new way that you create discovery rules. |

## Migrating Other RNA and RUA Settings

Various settings in the Version 4.10.3 system policy and system settings govern RNA data storage, impact flag correlation, operating system and service identity conflicts, RUA protocol monitoring, NetFlow settings, and so on.

### Migrating NetFlow Settings

The migration transfers the NetFlow-enabled devices you added using the Version 4.10.3 system settings to the Version 5.2 network discovery policy; you configure them on the Advanced tab. Your NetFlow monitoring and flow collection settings are also preserved in discovery rules as described in [Understanding How The Migration Creates Discovery Rules, page 5-14](#). Note that you do **not** need a license for NetFlow data collection in Version 5.2.

### Migrating General RNA Detection Policy Settings

The table below summarizes how the migration translates Version 4.10.3 RNA detection policy settings into Version 5.2 settings, most of which are in the network discovery policy. When you run the configuration import script, it overwrites your existing Version 5.2 settings with those in the import package.

**Table 5-7** Migrated RNA Detection Policy Settings

| Version 4.10.3 Setting             | Version 5.2 Setting                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Update Interval<br>Capture Banners | You now configure these settings as General Settings on the network discovery policy's Advanced tab. If you import configurations from more than one RNA detection policy, whether in one or different packages: <ul style="list-style-type: none"> <li>the new <b>Update Interval</b> is the lowest imported value</li> <li>if any of the Version 4.10.3 policies had <b>Capture Banners</b> enabled, it is enabled in Version 5.2</li> </ul> |
| Client Application Detection       | Application detection is now configured per discovery rule and cannot be disabled. You can, however, prevent NetFlow-detected applications from being added to the network map by logging connections only.                                                                                                                                                                                                                                    |

**Table 5-7** Migrated RNA Detection Policy Settings (continued)

| Version 4.10.3 Setting                                                          | Version 5.2 Setting                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Generate Hosts from NetFlow Data<br>Generate Services from NetFlow Data         | If you had these settings disabled in Version 4.10.3, when the migration creates discovery rules based on your NetFlow networks to monitor, an <b>Action of Log NetFlow Connections</b> ensures that NetFlow-discovered hosts and applications are <b>not</b> added to the network map, but NetFlow connections are still logged.                                                                                                                                                                                                                                                                                                                                                                   |
| Capture HTTP URLs Flow Data Mode<br>Combine Flows for Out-Of-Network Responders | <p>These settings are all logging-related (now handled by access control) and are <b>not</b> migrated to the network discovery policy:</p> <ul style="list-style-type: none"> <li>In Version 5.2, the <b>Capture HTTP URLs</b> setting becomes the <b>Maximum URL characters to store in connection events</b> setting, which you configure per access control policy and is enabled by default at 1024 characters.</li> <li>The other two Version 4.10.3 settings are always enabled in Version 5.2 and therefore you cannot configure them on the web interface.</li> </ul> <p>For more information, see <a href="#">Migrating RNA Settings into Rules and Logging Preferences, page 5-7</a>.</p> |

### Migrating RNA- and RUA-Related System Policy Settings

The table below summarizes how the migration translates Version 4.10.3 system policy configurations into Version 5.2 network discovery policy settings:

- The system policy's RNA Settings migrate to settings on the network discovery policy's Advanced tab.
- The system policy's RUA Settings migrate to settings on the network discovery policy's Users tab.

When you run the configuration import script, it overwrites your current Version 5.2 existing settings with those in the import package.

**Table 5-8** System Policy Settings Migrated to Network Discovery Policy Settings

| Version 4.10.3 System Policy Setting           | Version 5.2 Discovery Policy Setting         |
|------------------------------------------------|----------------------------------------------|
| RNA Data Storage Settings                      | Network Discovery Data Storage               |
| RNA Event Logging and Host Input Event Logging | Event Logging Settings                       |
| Vulnerabilities to use for Impact Assessment   | Vulnerabilities to use for Impact Assessment |
| Identity Conflict Settings                     | Identity Conflict Settings                   |
| Operating System and Service Identity Sources  | OS and Server Identity Sources               |
| RUA Detection Settings                         | Protocol Detection                           |

Note that the RNA data storage settings that combine flows and drop duplicate events are **not** migrated to the network discovery policy. Not only are these connection logging-related settings (now handled by access control), but in Version 5.2 these settings are always enabled and therefore you cannot configure them on the web interface.

In general, these settings and the way you configure them have not changed from version to version, although much of the discovery-related terminology has changed; see [New and Changed Terminology, page 1-2](#).

## Understanding Migrated Intrusion and Audit Events

Optionally, you can migrate legacy intrusion and audit events to your Version 5.2 Defense Center. Field names between the two versions correspond, but keep in mind the following points:

- Information in the intrusion event **Detection Engine** field is migrated to the Version 5.2 **Device** field.
- Any fields added to event tables since Version 4.10.3 are blank in imported legacy events.

Also keep in mind that the timestamps on legacy events will be “behind” newly generated events on the Version 5.2 Defense Center. Because the database is pruned by event timestamp, your migrated events will be pruned before those events.



**Tip**

If imported intrusion events do not display after you complete the import process, clear your browser cache and try again.

## Understanding Migrated Compliance Policies and Rules

In Version 5.2, the Policy & Response *compliance* features are collectively known as *correlation*. You can successfully migrate most compliance policies and rules to Version 5.2 correlation policies and rules. Most traffic profiles also migrate successfully.



**Note**

Compliance white lists are **not** migrated.

Version 4.10.3 configurations migrate regardless of whether they are activated; activated configurations in Version 4.10.3 are automatically activated in Version 5.2 by the migration process.

So that your Version 5.2 correlation configuration can behave equivalently to your Version 4.10.3 deployment, the migration must update configurations that use detection engine constraints. A Version 4.10.3 compliance rule based on an intrusion or flow event that uses a **Detection Engine** constraint becomes a Version 5.2 correlation rule based on an intrusion or connection event that uses a **Security Zone** constraint. Restricting correlation rules by zone preserves the Version 4.10.3 setting where a detection engine monitors the traffic flowing through a specified interface set. For more information, see [Understanding How Interface Sets Become Security Zones, page 5-12](#).

Also note that compliance conditions reflect terminology changes. For example, a Version 4.10.3 compliance condition with a **Service**, **Client Application**, or **Payload** constraint becomes a Version 5.2 condition with an Application Protocol, Client, or Web Application constraint. For more information, see [New and Changed Terminology, page 1-2](#).

The Policy & Responses configurations that you **cannot** migrate are detailed in the following table. Both the configuration export and import scripts warn you that these configurations will not be migrated, and give you a chance to exit the script.

**Table 5-9** *Unsupported Conditions in Compliance Rules and Traffic Profiles*

| You cannot migrate a... | Where...                                                                                                                                                 | Because...                                                                                                                                                                                                                                                                                  |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| compliance rule         | an <b>RNA event occurs</b> using a <b>Detection Engine</b> constraint                                                                                    | the migration script cannot create a Version 5.2 discovery-based correlation rule using a <b>Device</b> constraint until you add devices to the Defense Center, which you do after you run the import script. You can create these configurations after you complete the migration process. |
| compliance rule         | an <b>RNA event occurs</b> or a <b>flow event occurs</b> using an <b>Application Type</b> or <b>Payload Type</b> constraint                              | in Version 5.2, you cannot trigger correlation rules based on application categories and tags, which are the Version 5.2 analogs for application and payload types.                                                                                                                         |
| traffic profile         | a host profile qualification using a <b>Client Application</b> constraint where you specify one or more <b>Application Type</b> (other than <b>any</b> ) | in Version 5.2, you cannot track connections based on application categories and tags, which are the Version 5.2 analogs for application and payload types.                                                                                                                                 |
| traffic profile         | a host profile qualification using a <b>Client Application</b> constraint where you specify an <b>Application</b> of <b>any</b>                          | in Version 5.2, you cannot track connection based on a <b>Client</b> of <b>any</b> ; you must explicitly choose one or more client applications.                                                                                                                                            |

## Changes to eStreamer Syntax and Data Structures

With each release of the system software, several of the eStreamer data structures change. To determine whether each of the data structures your client currently receives is the current version of that structure, review the tables in the Host Discovery and Connection Data Blocks, Intrusion Event and Metadata Record Types, and Understanding Host Data Structures chapters in the [Version 5.2 Sourcefire 3D System eStreamer Integration Guide](#). If it is not, update your client to reflect the current structures.

In addition, you should review the Understanding the eStreamer Application Protocol chapter in detail to understand the new types of information available in Version 5.2 and how to request them.



### Note

Version 4.10.3 eStreamer settings on your appliances are **not** migrated. After you complete the migration process, you must re-enable the streaming of specific event types to eStreamer clients before you can request data, as well as add the client to the eStreamer server's peers database on the Defense Center. For more information, see the [Version 5.2 Sourcefire 3D System User Guide](#).

For a summary of the major changes to eStreamer, see the following sections.

### Series 2 Data Structures and Extended Requests

Series 2 data blocks were introduced in Version 5.0 and have a separate numbering system from series 1 data blocks. These blocks contain discovery and connection data and were previously known as RNA data structures.

Use *extended requests* to request information, such as Series 2 data blocks, that is not available from normal requests. Submit extended requests by setting bit 30 in the Event Stream Request message. When this bit is set, eStreamer responds with a list of available services. The client returns a Streaming Request message that indicates the service it wants to use, with a request list of event types and versions available from that service.

The eStreamer server sends messages in a bundle format when the client submits an extended request. The client responds with a NULL message to acknowledge receipt of an entire bundle. The client should not acknowledge receipt of individual messages in a bundle.

**Alternate Ports**

You can now configure eStreamer to use a port other than the primary management port.

**IPv6 and Geolocation**

Numerous data blocks now include source and destination countries for use with the geolocation feature. Also, all IP address fields now support both IPv4 and IPv6 addresses.